(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月4 日 (04.08.2005)

PCT

(10) 国際公開番号
WO 2005/071880 A1

(51) 国際特許分類[7]: H04L 9/32, G09C 1/00

(21) 国際出願番号: PCT/JP2005/001177

(22) 国際出願日: 2005 年1 月21 日 (21.01.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-016006 2004 年1 月23 日 (23.01.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 米澤 祥子 (YONEZAWA, Shoko) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 古川 潤 (FURUKAWA, Jun) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

(74) 代理人: 松本 正夫 (MATSUMOTO, Masao); 〒1710021 東京都豊島区西池袋二丁目３６番１０号 Tokyo (JP).

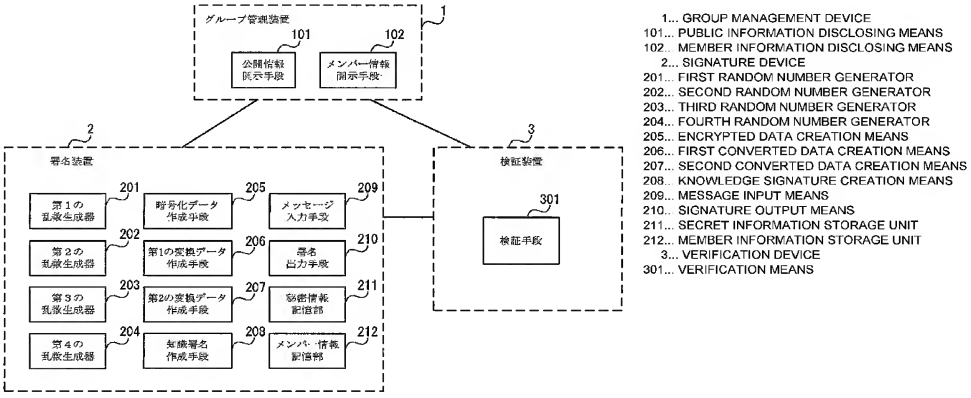
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE,

[続葉有]

(54) Title: GROUP SIGNATURE SYSTEM, METHOD, DEVICE, AND PROGRAM

(54) 発明の名称: グループ署名システム、方法、装置、およびプログラム



(57) Abstract: A signature device (2) encrypts a first element of a member certificate by using a first random number and public information disclosed by a group management device (1) so as to generate encrypted data. Moreover, the signature device (2) converts the first element by using a random number and the public information so as to create first and second converted data. Moreover, the signature device (2) creates knowledge signature data from which the first element, the second element, and the information on the signature key will not be known and outputs a group signature including it together with a message. A verification device (3) verifies whether the group signature has been created by using a member certificate and a signature key of a member registered in the group.

(57) 要約: 署名装置（２）は、メンバー証明書の第１の要素を第１の乱数とグループ管理装置（１）にて開示されている公開情報とを用いて暗号化して暗号化データを作成する。また、署名装置（２）は、第１の要素を乱数および公開情報を用いて変換して第１、第２の変換データを作成する。そして、署名装置（２）は、第１の要素、第２の要素、および署名鍵に関する情報を知られることのない知識署名データを作成し、それを含むグループ署名をメッセージと共に出力する。検証装置（３）は、メッセージおよびグループ署名と公開情報とから、グループ署名が、グループに登録されているいずれかのメンバーのメンバー証明書および署名鍵を用いて作成されたものか否かを検証する。

WO 2005/071880 A1

BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明細書

グループ署名システム、方法、装置、およびプログラム

技術分野

本発明は、グループに所属するメンバーが、グループのメンバーであることを証明するための署名を作成し、また検証するグループ署名システムに関し、特に、グループ管理者の処理権限を複数に分散する機能を有するグループ署名システムに関する。

背景技術

従来、この種のグループ署名システムは、複数のメンバーから構成されるグループにおいて、グループに所属する、あるユーザが署名を作成し、またその署名を検証するためのものである。そして、その署名は、署名者がグループのいずれかのメンバーであることは検証できるが、通常ではグループ内のどのメンバーであるかは分からないという性質のものである。ただし、その一方で、万が一のために、署名から実際の署名者を特定する機能（以下、追跡と称す）がグループ署名システムには備えられている。

一般に、グループ署名システムでは、グループ管理者と呼ばれるエンティティがグループ内に存在し、グループへの新たなメンバーの登録手続きおよび署名者の追跡を行う。その場合、グループ署名システムにおいて、グループへのメンバーの登録や、グループ署名の署名者追跡は、全てグループ管理者の権限で行われることとなる。このように、これら全ての権限を単一のグループ管理者に与えてしまうことがシステムの安全上好ましくない場合がある。

グループ管理者が不正を働こうとすれば、このグループ署名システムは不正を防止することができない。例えば、グループ管理者がメンバーを不正に追加し、そのメンバーを利用して、署名者の特定できない署名を作成することができてしまう。

このような不正が行なわれる可能性をできる限り低減し、グループ署名システ

ムの信頼性を向上させるために、単一のグループ管理者に全ての権限を与えることをせず、複数のエンティティでグループ管理者の役割を担うことが考えられる。

従来のグループ署名システムにおいては、グループ管理者の機能を、新たなユーザをグループに登録する権限を持つメンバー管理者と、グループ署名の署名者を特定する権限を持つメンバー追跡者に分割することが提案されている。G. Ateniese and R. de Medeiros, "Efficient Group Signatures without Trapdoors," In Advances in Cryptology--ASIACRYPT 2003, LNCS 2894, pp. 246-268, Springer-Verlag, 2003. (以下、文献1) および、G. Ateniese, J. Camenisch, M. Joye and G. Tsudik, "A Practical and Provable Secure Coalition-Resistant Group Signature Scheme," In Advances in Cryptology--CRYPTO2000, LNCS 1880, pp. 255-270, Springer-Verlag, 2000. (以下、文献2) で示されるグループ署名システムでは、このようなグループ管理者の分割が考慮されている。

また、そのメンバー管理者とメンバー追跡者の信頼性を更に向上させるために、メンバー管理者およびメンバー追跡者の各々の権限をさらに複数エンティティに分散し、複数のメンバー管理者あるいはメンバー追跡者が協力してそれら機能を果たすことも考えられている。

文献1にて提案された第1の従来技術において、メンバー管理者の用いる公開鍵と秘密鍵は、ElGamalによる"A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms" (IEEE Trans. on Information Theory, IT-31, 4, pp. 469-472) に記載されているように、有限体上の乗法群の離散対数問題に基づく暗号系から選択される。また、文献2で提案された第2の従来技術においては、メンバー管理者の用いる公開鍵と秘密鍵は、RSA暗号("A Method f

or Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120-126）のような暗号系に基づいて選択される。

文献１に記載された第１の従来技術のグループ署名システムは、公開情報開示手段と署名装置とを有している。図１３は、第１の従来技術のグループ署名システムにおける署名装置の構成を示すブロック図である。図１３を参照すると、署名装置は、第１の乱数生成器１２０１、第２の乱数生成器１２０２、第３の乱数生成器１２０３、第４の乱数生成器１２０４、第５の乱数生成器１２０５、第６の乱数生成器１２０６、第１の暗号化データ作成手段１２０７、第２の暗号化データ作成手段１２０８、第１の変換データ作成手段１２０９、第２の変換データ作成手段１２１０、知識署名作成手段１２１１、秘密情報記憶部１２１２、メンバー情報記憶部１２１３、メッセージ入力手段１２１４および署名出力手段１２１５から構成されている。

第１の乱数生成器１２０１は、第１の暗号化データ作成手段１２０７で使用する乱数を生成する。

第２の乱数生成器１２０２は、第２の暗号化データ作成手段１２０８で使用する乱数を生成する。

第３の乱数生成器１２０３は、第１の変換データ作成手段１２０９で使用する乱数を生成するとともに、その乱数をグループ署名の要素として署名出力手段１２１５に出力する。

第４の乱数生成器１２０４は、第２の変換データ作成手段１２１０で使用する乱数を生成するとともに、その乱数をグループ署名の要素として署名出力手段１２１５に出力する。

第５の乱数生成器１２０５は、第２の変換データ作成手段１２１０で使用する乱数を生成するとともに、その乱数をグループ署名の要素として署名出力手段１２１５に出力する。

第６の乱数生成器１２０６は、知識署名作成手段１２１１で使用する乱数を生成する。

第１の暗号化データ作成手段１２０７は、第１の乱数生成器１２０１で生成された乱数と、メンバー情報記憶部１２１２に記憶されているメンバー証明書の第１の要素とを入力として、メンバー証明書の第１の要素の暗号化データ（以下、第１の暗号化データと称す）を知識署名作成手段１２１１および署名出力手段１２１５に出力する。

第２の暗号化データ作成手段１２０８は、第２の乱数生成器１２０２で生成された乱数と、秘密情報記憶部１２１３に記憶されている署名鍵の変換データとを入力として、署名鍵の変換データの第１の要素の暗号化データ（以下、第２の暗号化データと称す）を知識署名作成手段９１１および署名出力手段１２１５に出力する。

第１の変換データ作成手段１２０９は、第３の乱数生成器１２０３で生成された乱数と、メンバー情報記憶部１２１２に記憶されているメンバー証明書の第１の要素を入力として、メンバー証明書の第１の要素の変換データ（以下、第１の変換データと称す）を知識署名作成手段１２１１および署名出力手段１２１５に出力する。

第２の変換データ作成手段１２１０は、第４の乱数生成器１２０４および第５の乱数生成器１２０５で生成された乱数と、メンバー情報記憶部１２１２に記憶されているメンバー証明書の第１の要素を入力として、メンバー証明書の第１の要素の変換データ（以下、第２の変換データと称す）を知識署名作成手段１２１１および署名出力手段１２１５に出力する。

知識署名作成手段１２１１は、メッセージ入力手段１２１４から入力されたメッセージ、第６の乱数生成器１２０６で生成された乱数、第１の暗号化データ、第２の暗号化データ、第１の変換データ、第２の変換データ、メンバー証明書の第１および第２の要素、および署名鍵を入力として、メンバー証明書および署名鍵に関する情報を漏らすことなくメンバー証明書および署名鍵を正しく所有していることを証明することのできる知識署名データを出力する。

メンバー情報記憶部１２１２は、グループ署名を発行するために用いるメンバー証明書を記憶する。メンバー証明書は第１の要素と第２の要素とからなる。

秘密情報記憶部１２１３は署名鍵を記憶する。

メッセージ入力手段１２１４は、署名を付加すべきメッセージを入力する。

署名出力手段１２１５は、メッセージ、第１の暗号化データ、第２の暗号化データ、第１の変換データ、第２の変換データ、第３の乱数、第４の乱数、第５の乱数、および知識署名データをグループ署名として出力する。

以上の構成により、第１の従来技術のグループ署名システムはグループ署名を作成することができる。

一方、文献２に記載された第２の従来技術のグループ署名システムは、グループ管理装置および署名装置を有している。

グループ管理装置は公開情報開示手段、メンバー情報開示手段、ＲＳＡ鍵生成手段、離散対数鍵生成手段、メンバー登録秘密情報記憶部、メンバー追跡秘密情報記憶部、およびメンバー登録手段を有している。そして、グループ管理装置は、グループメンバーの登録処理や、与えられた署名から実際の署名者の特定処理を行う。

公開情報開示手段は、システムで用いる公開情報をすべての装置に開示する。

メンバー情報開示手段は、メンバー登録手段で取得した署名装置に関する情報を開示する。

ＲＳＡ鍵生成手段は、ＲＳＡ暗号系による方法で公開鍵および秘密鍵を作成し、公開鍵を公開情報開示手段に出力し、秘密鍵をメンバー登録秘密情報記憶部に出力する。

離散対数鍵生成手段は、離散対数問題に基づく暗号系から公開鍵および秘密鍵を作成し、公開鍵を公開情報開示手段に出力し、秘密鍵をメンバー追跡秘密情報記憶部に出力する。

メンバー登録秘密情報記憶部は、ＲＳＡ鍵生成手段で作成した秘密鍵を記憶する。

メンバー追跡秘密情報記憶部は、離散対数鍵生成手段で作成した秘密鍵を記憶する。

メンバー登録手段は、メンバー登録秘密情報記憶部に記憶された秘密鍵を入力として、グループ署名を作成するのに必要なメンバー証明書を署名装置に対して出力する。

一方、署名装置は、グループ管理装置から取得したメンバー証明書を用いてグループ署名を作成する。

そして、第２の従来技術によるグループ管理装置はメンバー管理装置とメンバー追跡装置に分割されてもよい。その場合、メンバー管理装置はＲＳＡ鍵生成手段、メンバー登録秘密情報記憶部、およびメンバー登録手段を有し、メンバー追跡装置は離散対数鍵生成手段、メンバー追跡秘密情報記憶部を有することとなる。

第１の問題点は、第１の従来技術において、グループ管理装置をメンバー管理装置とメンバー追跡装置に機能分割すると、メンバー管理装置が実際の署名者を特定する機能を有することとなってしまう点である。

第１の従来技術では、第１の変換データ作成手段１２０９で作成される第１の変換データは、第３の乱数生成器１２０３で生成される乱数（以下、第３の乱数と称す）とメンバー証明書の第１の要素とに依存する確定的な値であり、かつ第３の乱数は後にグループ署名の要素として公開される。そのため、メンバー管理装置は、開示されたすべてのメンバー証明書の情報と、グループ署名の要素として開示された第３の乱数とを入力として、全てのメンバー証明書について総当りで第１の変換データ作成手段１２０９と同じ変換を行い、署名装置から出力されたグループ署名に含まれた第１の変換データと一致する値が得られたときのメンバー証明書の持ち主を調べれば、署名者を特定できてしまう。

第２の問題点は、第２の従来技術において、メンバー管理装置の処理権限を複数エンティティに分散する場合、複数のエンティティに大きな負荷がかかり、効率的でないという点である。

第２の従来技術では、メンバー管理装置の用いる秘密鍵はＲＳＡ暗号系に基づいて選択されているが、一般にＲＳＡ暗号系の分散計算は複雑で、計算量が大きいことが知られている。そのため、この大きな計算量による負荷が複数のエンティティにかかることとなる。

本発明の目的は、グループ署名からメンバー証明書に関する情報を秘匿できるグループ署名を提供し、また、グループ管理装置の機能を安全確実にメンバー管理装置とメンバー追跡装置に分割することができ、さらに、メンバー管理装置およびメンバー追跡装置の機能を効率良く複数のエンティティに分散させることの

できるグループ署名システムを提供することである。

発明の開示

上記目的を達成するために、本発明のグループ署名システムは、署名者がグループに登録されたメンバーであることを証明することのできるグループ署名を作成し、また、作成された前記グループ署名の前記署名者が前記グループのメンバーであるか否か確認するグループ署名システムであって、

システム内で共通に利用する公開情報を他の装置から参照可能に開示するグループ管理装置と、

第１の要素および第２の要素を含むメンバー証明書を記憶しており、前記第１の要素を第１の乱数と前記グループ管理装置にて開示されている前記公開情報とを用いて暗号化して暗号化データを作成し、前記第１の要素を第２の乱数および前記公開情報を用いて変換して第１の変換データを作成し、前記第１の要素を第３の乱数および前記公開情報を用いて変換して第２の変換データを作成し、署名を付加すべきメッセージ、第４の乱数、前記暗号化データ、前記第１の変換データ、前記第２の変換データ、署名の作成に用いる秘密鍵である署名鍵、前記第１の要素、および前記第２の要素から、知識署名データを作成し、前記暗号化データ、前記第１の変換データ、前記第２の変換データ、および前記知識署名データをグループ署名として前記メッセージと共に出力する署名装置と、

メッセージおよびグループ署名と、前記グループ管理装置にて開示されている前記公開情報とから、前記グループ署名が、前記グループに登録されているいずれかのメンバーのメンバー証明書に含まれる第１の要素および第２の要素と前記署名鍵を用いて作成されたものか否かを検証する検証装置とを有している。

また、前記署名装置は、前記暗号化データ、前記第１の変換データ、および前記第２の変換データが同じ値を元に作成されていることを証明可能でありかつ前記第１の要素、前記第２の要素、および前記署名鍵に関する情報を知られることのないデータとして、前記知識署名データを作成し、

前記検証装置は、グループ署名が、前記グループに登録されているいずれかのメンバーのメンバー証明書に含まれる第１の要素および第２の要素と前記署名鍵

を用いて作成されたものか否かを、前記第１の要素、前記第２の要素、および前記署名鍵に関する情報を用いることなく、検証することとしてもよい。

また、新たなメンバーを前記グループに登録するとき、素数を位数とする有限体の元となるようにメンバー登録秘密鍵を選び、前記メンバー登録秘密鍵を離散対数とし、有限体上の乗法群の元であるメンバー登録公開鍵を前記メンバー登録秘密鍵から求め、前記メンバー登録公開鍵を公開情報として前記グループ管理装置に通知し、前記メンバー登録秘密鍵を自身で記憶すると共に、該メンバー登録秘密鍵を用いてメンバー証明書を作成し、前記署名装置に通知するメンバー管理装置をさらに有することとしてもよい。

また、前記メンバー証明書は、前記署名鍵を離散対数とする、前記署名鍵の変換データに対して前記メンバー登録秘密鍵を用いて作成したＮｙｂｅｒｇ－Ｒｕｅｐｐｅｌ署名であるとしてもよい。

また、前記グループ管理装置は、前記公開情報に加えて、前記メンバー管理装置から通知された前記メンバー情報を他の装置から参照可能に開示するものとしてもよい。

また、本発明のシステムは、新たなメンバーを前記グループに登録するとき、素数を位数とする有限体の所定の元の、複数に分散された値のうちの１つを自身の分散メンバー登録秘密鍵として割り当て、前記分散メンバー登録秘密鍵を自身で記憶すると共に、前記元を離散対数とする値をメンバー登録公開鍵とする、複数のメンバーサブ管理装置をさらに有し、

前記署名装置は、複数の前記メンバーサブ管理装置と通信することによりメンバー証明書を取得し、

前記グループ管理装置は、前記メンバー登録公開鍵を取得するものとしてもよい。

また、本発明のシステムは、素数を位数とする有限体の元となるようにメンバー追跡秘密鍵を選び、前記メンバー追跡秘密鍵を離散対数とし、有限体上の乗法群の元であるメンバー追跡公開鍵を前記メンバー追跡秘密鍵から求め、前記メンバー追跡公開鍵を前記公開情報として前記グループ管理装置に通知し、前記メンバー追跡秘密鍵を自身で記憶しておき、グループ署名の署名者を特定するとき、

前記グループ署名に含まれている暗号化データを前記メンバー追跡秘密鍵を用いて復号し、復号結果と前記グループ管理装置にて開示されているいずれかの前記メンバー証明書の第１の要素とが一致すれば該メンバー証明書のメンバーを署名者と特定するメンバー追跡装置をさらに有し、

前記グループ管理装置は前記メンバー証明書を前記メンバー情報として開示しており、

前記署名装置は前記第１の要素を暗号化して前記暗号化データを作成するとき前記公開情報として前記メンバー追跡公開鍵を用いることとしてもよい。

また、自身の分散メンバー追跡秘密鍵が、素数を位数とする有限体の元の複数に分散された値のうちの自身に割り当てる１つであり、メンバー追跡公開鍵が、前記有限体の元を離散対数とし、有限体上の乗法群の元となるように、前記分散メンバー追跡秘密鍵を求め、前記分散メンバー追跡秘密鍵を自身で記憶する複数のメンバーサブ追跡装置をさらに有し、

前記署名装置は前記第１の要素を暗号化して前記暗号化データを作成するとき前記公開情報として前記メンバー追跡公開鍵を用い、

前記グループ管理装置は前記メンバー証明書を前記メンバー情報として開示しており、

グループ署名の署名者を特定するとき、前記メンバーサブ追跡装置の各々が前記グループ署名に含まれている暗号化データに対して自身の前記分散メンバー追跡秘密鍵を用いて所定の計算をした結果から求まる復号結果と、前記グループ管理装置にて開示されているいずれかの前記メンバー証明書の第１の要素とが一致すれば該メンバー証明書のメンバーを署名者と特定することとしてもよい。

また、前記有限体上の乗法群に代えて楕円曲線上の有限群を用いることとしてもよい。

したがって、本発明によれば、署名装置が、メンバー証明書に関する情報を、グループ署名の要素として開示されない乱数を用いて秘匿することができる。また、メンバー管理装置の機能は複数のメンバーサブ管理装置に分散され、複数のメンバーサブ管理装置がメンバー証明書を計算するために使用する秘密鍵は、離散対数問題に基づく暗号系から選ばれる。また、メンバー追跡装置の機能は複数

のメンバーサブ追跡装置に分散され、複数のメンバーサブ追跡装置が署名者の特定に用いる秘密鍵は、離散対数問題に基づく暗号系から選ばれる。

図面の簡単な説明

図１は、第１の実施形態のグループ署名システムの構成例を示すブロック図である。

図２は、第１の実施形態のグループ署名システムの他の構成例を示すブロック図である。

図３は、第１の実施形態のグループ署名システムのさらに他の構成を示すブロック図である。

図４は、第１の実施形態の署名装置を構成する各ブロック間の関係を示す図である。

図５は、第１の実施形態の署名装置およびメンバー管理装置を構成する各ブロック間の関係を示す図である。

図６は、第１の実施形態の検証装置内のブロックと他の装置との関係を示す図である。

図７は、第１の実施形態のメンバー管理装置を構成する各ブロック間の関係を示す図である。

図８は、第１の実施形態のメンバー追跡装置を構成する各ブロック間の関係を示す図である。

図９は、第１の実施形態のメンバー追跡装置を構成する各ブロック間の関係を示す図である。

図１０は、第１の実施形態によるグループ署名システムのメンバー登録時の動作を示すフローチャートである。

図１１は、第１の実施形態による署名装置のグループ署名作成時の動作を示すフローチャートである。

図１２は、第２の実施形態のグループ署名システムの構成例を示すブロック図である。

図１３は、第１の従来技術のグループ署名システムにおける署名装置の構成を

示すブロック図である。

発明を実施するための最良の形態

本発明の一実施形態について図面を参照して詳細に説明する。

図１は、第１の実施形態のグループ署名システムの構成例を示すブロック図である。図１を参照すると、第１の実施形態のグループ署名システムは、グループ管理装置１、署名装置２、および検証装置３を有している。

なお、他の構成例として、第１の実施形態のグループ署名システムは、図１の構成に加えてメンバー管理装置を有してもよい。図２は、第１の実施形態のグループ署名システムの他の構成例を示すブロック図である。図２を参照すると、第１の実施形態のグループ署名システムは、図１の構成に加えて、メンバー管理装置４を有している。

さらに他の構成例として、第１の実施形態のグループ署名システムは、図２の構成に加えてメンバー追跡装置５を有してもよい。図３は、第１の実施形態のグループ署名システムのさらに他の構成を示すブロック図である。図３を参照すると、第１の実施形態のグループ署名システムは、図２の構成に加えて、メンバー追跡装置５を有している。

以下、メンバー登録機能とメンバー追跡機能の各々をグループ管理装置１から分割した図３のシステム構成例を用いて説明する。ただし、本発明はその構成に限定されるものではなく、それら機能を分割しない構成にも適用可能である。

図３を参照すると、グループ管理装置１は、公開情報開示手段１０１、メンバー情報開示手段１０２、および前処理手段１０３を有しており、システム全体で用いる公開情報を作成し、開示する。

署名装置２は、第１の乱数生成器２０１、第２の乱数生成器２０２、第３の乱数生成器２０３、第４の乱数生成器２０４、暗号化データ作成手段２０５、第１の変換データ作成手段２０６、第２の変換データ作成手段２０７、知識署名作成手段２０８、メッセージ入力手段２０９、署名出力手段２１０、秘密情報記憶部２１１、メンバー情報記憶部２１２、登録手段２１３、および第５の乱数生成器２１４を有しており、メンバー登録の後、グループ署名を作成する。

検証装置３は検証手段３０１を有しており、与えられたグループ署名の正当性を確認する。

メンバー管理装置４は、離散対数鍵生成手段４０１、メンバー登録秘密情報記憶部４０２、メンバー登録手段４０３、第１の乱数生成器４０４、第２の乱数生成器４０５を有しており、グループメンバーの登録処理を行う。

メンバー追跡装置５は、離散対数鍵生成手段５０１、メンバー追跡秘密情報記憶部５０２、メンバー追跡手段５０３、および乱数生成器５０４を有しており、与えられたグループ署名から実際の署名者を特定するメンバー追跡機能を有している。

グループ管理装置１において公開情報開示手段１０１は、前処理手段１０３、離散対数鍵生成手段４０１、離散対数鍵生成手段５０１から出力された各種の公開情報を記憶し、すべての装置が自由に参照できるように開示する。

メンバー情報開示手段１０２は、メンバー管理装置４のメンバー登録手段４０３と署名装置２の登録手段２１３とが互いに通信することにより作成されたメンバー情報を記憶し、すべての装置が自由に参照できるように開示する。

前処理手段１０３は、本システムで用いる共通の定数を予め定め、それを公開情報開示手段１０１に出力する。

図４は、第１の実施形態の署名装置を構成する各ブロック間の関係を示す図である。図５は、第１の実施形態の署名装置およびメンバー管理装置を構成する各ブロック間の関係を示す図である。

まず、図４において、第１の乱数生成器２０１は、暗号化データ作成手段２０５で使用する第１の乱数を生成する。

同様に、第２の乱数生成器２０２は、第１の変換データ作成手段２０６で使用する第２の乱数を生成する。第３の乱数生成器２０３は、第２の変換データ作成手段２０７で使用する第３の乱数を生成する。第４の乱数生成器２０４は、知識署名作成手段２０８で使用する第４の乱数を生成する。

暗号化データ作成手段２０５は、第１の乱数生成器２０１で生成した第１の乱数と、メンバー情報記憶部２１２に記憶されているメンバー証明書の第１の要素とを入力として、メンバー証明書の第１の要素を暗号化し、得られた暗号化デー

タを知識署名作成手段２０８および署名出力手段２１０に出力する。

第１の変換データ作成手段２０６は、第２の乱数生成器２０２で生成した第２の乱数と、メンバー情報記憶部２１２に記憶されているメンバー証明書の第１の要素とを入力として、メンバー証明書の第１の要素の変換データ（以下、第１の変換データと称す）を知識署名作成手段２０８および署名出力手段２１０に出力する。

第２の変換データ作成手段２０７は、第３の乱数生成器２０３で生成した第３の乱数と、メンバー情報記憶部２１２に記憶されているメンバー証明書の第１の要素とを入力として、メンバー証明書の第１の要素の変換データ（以下、第２の変換データと称す）を知識署名作成手段２０８および署名出力手段２１０に出力する。

知識署名作成手段２０８は、メッセージ入力手段２０９から入力されたメッセージ、第４の乱数生成器２０４で生成した第４の乱数、暗号化データ、第１の変換データ、第２の変換データ、秘密情報記憶部２１１に記憶されている署名鍵、メンバー情報記憶部２１２に記憶されているメンバー証明書の第１および第２の要素、公開情報開示手段１０１にて開示されている公開情報を入力として、メンバー証明書および署名鍵を所持していることを示す知識署名データを出力する。

メッセージ入力手段２０９は、署名を付加すべきメッセージを知識署名作成手段２０８および署名出力手段２１０に出力する。

署名出力手段２１０は、メッセージ入力手段２０９から入力されたメッセージ、暗号化データ、第１の変換データ、第２の変換データ、知識署名データをグループ署名として出力する。

秘密情報記憶部２１１は、署名に用いる秘密鍵である署名鍵を記憶する。

メンバー情報記憶部２１２は、メンバー管理装置４のメンバー登録手段４０３との通信を用いて取得したメンバー証明書を記憶する。

図５において、登録手段２１３は、メンバー管理装置４のメンバー登録手段４０３と通信を行い、また第５の乱数生成器２１４から出力された第５の乱数を入力として、メンバー管理装置４の署名を表すメンバー証明書と署名装置２の秘密情報である署名鍵とを取得し、前記メンバー証明書をメンバー情報記憶部２１２

に、前記署名鍵を秘密情報記憶部２１２に、それぞれ出力する。第５の乱数生成器２１４は、登録手段２１３に入力する第５の乱数を生成する。

図６は、第１の実施形態の検証装置内のブロックと他の装置との関係を示す図である。

検証手段３０１は、与えられたグループ署名と、グループ管理装置１の公開情報開示手段１０１にて開示された公開情報とを入力として、グループ署名が署名装置２の署名出力手段２１０から正しく出力されたものか否か検証する。そして、検証手段３０１は、グループ署名が署名出力手段２１０から正しく出力されたものであるときのみ、そのグループ署名を受理し、そうでないときには、署名を不受理とする。

これにより、検証手段２１０は、与えられたグループ署名が、ある署名装置が正しいメンバー証明書および署名鍵を使用して作成した正当なグループ署名であるか否かを検証し、正当なグループ署名であれば受理して署名受理の旨を出力し、そうでなければ不受理とし、署名不受理の旨を出力する。

図７は、第１の実施形態のメンバー管理装置を構成する各ブロック間の関係を示す図である。

図７を参照すると、離散対数鍵生成手段４０１は、第１の乱数生成器４０４から乱数を受け、その乱数を用いて、有限体上の乗法群の離散対数問題に基づく公開鍵と秘密鍵を計算し、秘密鍵をメンバー登録秘密鍵としてメンバー登録秘密情報記憶部４０２に記録し、公開鍵をメンバー登録公開鍵としてグループ管理装置１の公開情報開示手段１０１に出力する。

メンバー登録秘密情報記憶部４０２は、離散対数鍵生成手段４０１で作成した秘密鍵を記憶する。

第１の乱数生成器４０４は、離散対数鍵生成手段４０１に乱数を出力する。

図５を参照すると、メンバー登録手段４０３は、署名装置２の登録手段２１３と通信し、また第２の乱数生成器４０５からの乱数と、メンバー登録秘密情報記憶部４０２に記憶された秘密鍵とを入力として、署名装置２に対して第１の要素と第２の要素からなるメンバー証明書を発行し、また署名装置２との通信で得た署名装置２のメンバー情報をメンバー情報開示手段１０２に出力する。メンバー

証明書は、グループのメンバーであることを証明する情報であり、署名装置２がグループ署名を発行するときに用いられる。

第２の乱数生成器４０５は、メンバー登録手段４０３に乱数を出力する。

図８および図９は、第１の実施形態のメンバー追跡装置を構成する各ブロック間の関係を示す図である。

図８を参照すると、離散対数鍵生成手段５０１は、乱数生成器５０４から乱数を受け、その乱数を用いて、有限体上の乗法群の離散対数問題に基づく公開鍵と秘密鍵を計算し、秘密鍵をメンバー追跡秘密鍵としてメンバー追跡秘密情報記憶部５０２に記録し、公開鍵をメンバー追跡公開鍵としてグループ管理装置１の公開情報開示手段１０１に出力する。

メンバー追跡秘密情報記憶部５０２は、離散対数鍵生成手段５０１で作成した秘密鍵を記憶する。

乱数生成器５０４は、離散対数鍵生成手段５０１に乱数を出力する。

図９を参照すると、メンバー追跡手段５０３は、検証手段３０１で受理されたグループ署名と、メンバー情報開示手段１０２にて開示されているメンバー情報と、メンバー追跡秘密情報記憶部５０２に記憶されている秘密鍵を入力として、グループ署名の署名者を特定する。

以下、第１の実施形態のグループ署名システムの詳細動作について説明する。

まず最初に前処理として、前処理手段１０３が本システムで共通に用いる公開パラメータを設定する。ここで設定されたパラメータは、後に行われる、署名装置２、メンバー管理手段４、およびメンバー追跡手段５における鍵生成に用いられる。

前処理においては、まず第１の素数ｐ，第２の素数ｑ，第３の素数Ｐを選ぶ。このとき、ｐ，ｑ，Ｐは、

ｑ｜ｐ－１，　ｐ｜Ｐ－１

の関係を満たすように選ぶ。

ｐ，ｑ，Ｐのビット数は、それぞれ

｜ｑ｜≧１６０，｜ｐ｜≧１０２４，｜Ｐ｜≧１０２４

が推奨される。

ここで、ｐを位数とする乗法群Z_p^*の、位数ｑの部分群Ｇｑを考える。また、Ｐを位数とする乗法群Z_P^*の、位数ｐの部分群Ｇｐを考える。

そして、Ｇｐから第１の生成元ｇ、第２の生成元ｈ、および第３の生成元ｆを選ぶ。このとき、$g^{\alpha 1} h^{\alpha 2} f^{\alpha 3} = 1$となる自明でない$\alpha 1$，$\alpha 2$，$\alpha 3$を知らないように、ｇ，ｈ，ｆを選ぶ。

同様に、Ｇｐから第４の生成元Ｇ、および第５の生成元Ｈを選ぶ。このとき、$G^{\beta 1} H^{\beta 2} = 1$となる自明でない$\beta 1$，$\beta 2$を知らないように、Ｇ，Ｈを選ぶ。

また、任意のビット列をｋビットに変換する衝突困難ハッシュ関数

$\mathcal{H}$

を選ぶ。ｋの値は１６０が推奨される。

そして、最後に、第１の素数ｐ、第２の素数ｑ、第３の素数Ｐ、第１の生成元ｇ、第２の生成元ｈ、第３の生成元ｆ、第４の生成元Ｇ、第５の生成元Ｈ、および衝突困難ハッシュ関数

$\mathcal{H}$

を公開情報開示手段１０１に出力する。

次に、メンバー管理装置４は、離散対数鍵生成手段４０１により、メンバー登録手段４０３で用いる離散対数問題に基づく秘密鍵と公開鍵の対を作成する。この秘密鍵がメンバー登録秘密鍵であり、公開鍵がメンバー登録公開鍵である。

これらの作成において、第１の乱数生成器４０４は前処理手段１０３で選んだ第２の素数ｑを位数とする有限体Ｚｑからメンバー登録秘密鍵υをランダムに選び、離散対数鍵生成手段４０１に入力する。次に、離散対数鍵生成手段４０１は、第２の生成元ｈとメンバー登録秘密鍵υから、メンバー登録公開鍵

$y = h^{\upsilon} \bmod p$

を計算する。すなわち、有限体上の乗法群の離散対数問題に基づく公開鍵と秘密鍵の計算においては、秘密鍵が、素数を位数とする有限体の任意の元であり、公開鍵が、その秘密鍵を離散対数とする値となるように、公開鍵および秘密鍵を選ぶこととなる。

最後に、メンバー登録公開鍵ｙを公開情報開示手段１０１に出力し、メンバー登録秘密鍵υをメンバー管理秘密情報記憶部４０２に厳重に保存する。

同様に、メンバー追跡装置５は、離散対数鍵生成手段５０１により、メンバー追跡手段５０３で用いる離散対数問題に基づく秘密鍵と公開鍵の対を作成する。この秘密鍵がメンバー追跡秘密鍵であり、公開鍵がメンバー追跡公開鍵である。

これらの作成において、乱数生成器５０４は前処理手段１０３で作成した第２の素数ｑを位数とする有限体Ｚｑからメンバー追跡秘密鍵εをランダムに選び、離散対数鍵生成手段５０１に入力する。次に、離散対数鍵生成手段５０１は、第１の生成元ｇとメンバー追跡秘密鍵εから、メンバー追跡公開鍵

$$e = g^{\varepsilon} \bmod p$$

を計算する。最後に、メンバー追跡公開鍵ｅを公開情報開示手段１０１に出力し、メンバー追跡秘密鍵εをメンバー追跡秘密情報記憶部５０２に厳重に保存する。

以上の処理は、システムが動作を開始する際、もしくはシステムを初期化する際に行われる。

前処理および鍵生成の後、署名装置２はメンバー管理装置４との間で通信を行い、後に署名発行に使用する署名鍵とメンバー証明書を取得する。メンバー証明書は、署名装置２の第５の乱数生成器２１４が選んだ乱数を署名鍵とし、その署名鍵の変換データに対して、メンバー管理装置４が計算したメンバー管理秘密鍵を用いて、例えば、ＮｙｂｅｒｇとＲｕｅｐｐｅｌによる署名方式（“Ｍｅｓｓａｇｅ Ｒｅｃｏｖｅｒｙ ｆｏｒ Ｓｉｇｎａｔｕｒｅ Ｓｃｈｅｍｅｓ Ｂａｓｅｄ ｏｎ ｔｈｅ Ｄｉｓｃｒｅｔｅ Ｌｏｇａｒｉｔｈｍ Ｐｒｏｂｌｅｍ，” Ａｄｖａｎｃｅｓ ｉｎ Ｃｒｙｐｔｏｌｏｇｙ － ＥＵＲＯＣＲＹＰＴ ‘９４， ｐｐ．１８２－１９３）に従って作成した署名データである。この署名データはＮｙｂｅｒｇ－Ｒｕｅｐｐｌ署名と称される。このメンバー証明書は第１の要素および第２の要素で構成される。

以下、メンバー証明書の発行を行うメンバー登録手段４０３および登録手段２１３の動作の例を示す。

図１０は、第１の実施形態によるグループ署名システムのメンバー登録時の動作を示すフローチャートである。

図１０を参照すると、署名装置２の登録手段２１３は、まずステップＡ１０１で、第５の乱数生成器２１４で生成された、第２の素数ｑを位数とする有限体Ｚｑのいずれかの元σを署名装置２の署名鍵として受け取る。

次に、ステップＡ１０２で、署名鍵σの変換データとして

$I_U = g^{\sigma} \bmod p$

を計算する。

また、ステップＡ１０３で、署名鍵σが第１の生成元ｇに関する署名鍵の変換データI_Uの離散対数であることの知識署名データspk_Uを計算する。知識署名データspk_Uは、Ｓｃｈｎｏｒｒの“Ｅｆｆｉｃｉｅｎｔ　Ｓｉｇａｎｔｕｒｅ　Ｇｅｎｅｒａｔｉｏｎ　ｂｙ　Ｓｍａｒｔ　Ｃａｒｄｓ”（Ｊｏｕｒｎａｌ　ｏｆ　Ｃｒｙｐｔｏｌｏｇｙ，４，３，ｐｐ．１６１－１７４）に示された方法を用いて、次のように作成することができる。

有限体Ｚｑから乱数λを選び、（ｃ，ｓ）を次のように計算する。

$$c := \mathcal{H}\left(g \,\|\, I_U \,\|\, g^{\lambda}\right)$$

$$s := \lambda - c\sigma \bmod q$$

この計算で得られた

$spk_U = (c, s)$

が知識署名データとなる。

また、ステップＡ１０４で、署名鍵の変換データI_Uと知識署名データspk_Uを署名装置２が正しく作成したことを示す本人確認データを作成する。このデータには、署名鍵の変換データと知識署名データとの連結データに対するデジタル署名などを使用できる。

デジタル署名関数Sig_Uを用いる場合、本人確認データは

$S_U = Sig_U(I_U \| spk_U)$

となる。デジタル署名関数Sig_Uには、ＤＳＡ署名やＲＳＡ署名などの署名アルゴリズムを使用することができる。

そして、署名装置２は変換データI_U，知識署名データspk_U，本人確認データS_Uをメンバー管理装置４に送信する。

メンバー管理装置４は、知識署名データｓｐｋ$_U$と本人確認データＳ$_U$が正しいか否か検証する（ステップＡ１０５）。知識署名データｓｐｋ$_U$の正しさは次の等式が成り立つ否かを確認することにより検証できる。

$$c = \mathcal{H}(g \| I_U \| I_U^{\upsilon} g^{\rho})$$

一方、デジタル署名Ｓ$_U$の正しさは、Ｓｉｇ$_U$に対応するデジタル署名検証関数Ｖｅｒ$_U$を用いて、

Ｖｅｒ$_U$（Ｓ$_U$，Ｉ$_U$‖ｓｐｋ$_U$）＝１

が成り立つか否かを確認することにより検証できる。

両者ともが検証を通過したら処理が継続される。いずれか１つでも検証を通過できなければ、処理が中断される。

検証を通過した後、メンバー管理装置４のメンバー登録手段４０３は、ランダムに選んだ第２の素数ｑを位数とする有限体Ｚｑの元ρを第２の乱数生成器４０５から受け取る（ステップＡ１０６）。

次に、ステップＡ１０７で、メンバー登録手段４０３は、受け取った乱数ρとメンバー管理秘密情報記憶部４０２に記憶されたメンバー管理秘密鍵υと公開情報開示手段１０１に開示された第２の生成元ｈとを使って、メンバー証明書（ｒ，ξ）を次のように計算する。

$$r := I_U h^{\rho} \bmod p$$

$$\xi := \rho - r\upsilon \bmod q$$

そして、メンバー管理装置４は計算で得たメンバー証明書（ｒ，ξ）を署名装置２に送信する。

ステップＡ１０８において、署名装置２は受け取ったメンバー証明書（ｒ，ξ）が正しく作られているか否かを検証する。この検証は、次の等式が成り立つか否かを確認することにより行う。

$r = y^r g^{\sigma} h^{\xi}$

検証を通過したら、署名装置２は、メンバー管理装置４にメンバー証明書を確認できた旨を通知する（ステップＡ１０９）。そして署名装置２は、署名鍵σを秘密情報記憶部２１１に保存し、メンバー証明書（ｒ，ξ）をメンバー情報記憶

部２１２に保存する（ステップＡ１１０）。

また、メンバー管理装置４は、ステップＡ１０９で通知された検証成功通知を受けとると、署名装置２を示すメンバーリストとして、署名鍵の変換データI_U、知識署名データspk_U、署名装置２に送信したメンバー証明書（ｒ，ξ）、および本人確認データS_Uをメンバー情報開示手段１０２に出力する（ステップＡ１１１）。この登録処理は署名装置毎に行う。

メンバー証明書および署名鍵の作成が済んだ署名装置２は、メッセージ入力手段２０９から入力されたグループ署名を施すべき電子文書メッセージｍに対し、グループ署名を次のように作成する。

図１１は、第１の実施形態による署名装置のグループ署名作成時の動作を示すフローチャートである。

図１１を参照すると、ステップＡ２０１で、第１の乱数生成器２０１が有限体Ｚｑから第１の乱数τを生成し、第２の乱数生成器２０２が有限体Ｚｑから第２の乱数ωを生成し、第３の乱数生成器２０３が有限体Ｚｐから第３の乱数ａを生成する。

次に、ステップＡ２０２で、暗号化データ作成手段２０５は、第１の乱数τとメンバー証明書の第１の要素ｒとメンバー追跡公開鍵ｅを入力として、

$$g' := g^{\tau} \bmod p$$

$$e' := r^{-1} e^{\tau} \bmod p$$

を計算する。そして、この（ｇ′，ｅ′）を、メンバー証明書の第１の要素ｒの暗号化データと呼ぶ。

次に、ステップＡ２０３で、第１の変換データ作成手段２０６は、第２の乱数ωとメンバー証明書の第１の要素ｒを入力として、

$$h' := y^{r} f^{\omega} \bmod p$$

を計算する。このｈ′をメンバー証明書の第１の要素ｒの第１の変換データと呼ぶ。

同様に、ステップＡ２０４で、第２の変換データ作成手段２０７は、第３の乱数ａとメンバー証明書の第１の要素ｒを入力として、

$$J := G^{r} H^{a} \bmod P$$

を計算する。このＪをメンバー証明書の第１の要素ｒの第２の変換データと呼ぶ。

これらの暗号化および変換データは乱数を入力として作成しているので、変換データが公開されても、メンバー証明書の第１の要素ｒに関する情報は一切知られることがない。

これらの処理により、メンバー証明書の第１の要素ｒは、乱数を用いて秘匿されたことになる。

次に、ステップＡ２０５で、知識署名作成手段２０８が知識署名データを作成する。

知識署名データは、メッセージｍを入力として、第１の変換データｈ′および第２の変換データＪがメンバー証明書の第１の要素ｒの正しい変換であり、かつｈ′とＪが共に同じメンバー証明書の第１の要素ｒを変換していること、メンバー証明書（ｒ，ξ）をメンバー管理装置４と通信して正しく取得したこと、およびメンバー証明書（ｒ，ξ）に対応する署名鍵σを知っていること、暗号化データ（ｇ′，ｅ′）がメンバー証明書の第１の要素ｒをメンバー追跡公開鍵ｅで正しく暗号化したものであることを、メンバー証明書（ｒ，ξ）、署名鍵σ、第１の乱数τ、第２の乱数ω、および第３の乱数ａに関する情報を漏らさずに証明することのできるデータである。

本実施形態では、知識署名データは、等式

$$\begin{cases} g' = g^{\tau} \bmod p \\ e' = r^{-1} e^{\tau} \bmod p \\ h' = y^{r} f^{\omega} \bmod p \\ J = G^{r} H^{a} \bmod p \\ e' h' = f^{\omega} g^{-\sigma} h^{-\xi} e^{\tau} \bmod p \\ r \in [0, p-1] \end{cases}$$

を満たす（ｒ，ξ，σ，τ，ω，ａ）を知っていることを、（ｒ，ξ，σ，τ，ω，ａ）を明かさないままで（すなわち、これらの情報を漏らすことなく）、証明する。

まず最初に、１≦ｊ≦ｋとして、０からｐ－１の間から乱数φ2j-1を選ぶ。ま

た、

$\phi_{2j} := \phi_{2j-1} - p$

とおく。

そして、次に、

$r + \phi_{2j} \in [0, p-1]$

が成り立つか否か確認する。このとき、

$r + \phi_{2j-1} \notin [0, p-1]$ かつ $r + \phi_{2j} \in [0, p-1]$

であれば、ϕ_{2j-1}とϕ_{2j}を交換し、

$r + \phi_{2j-1} \in [0, p-1]$

となるように値を置き換える。

また、有限体Ｚｑから乱数$\psi 2j-1$, $\psi 2j$を、有限体Ｚｐから乱数η_{2j-1}, η_{2j}をランダムに選ぶ。これらの乱数を用いて、１≦ｊ≦ｋについて次の値を計算する。

$$V_j := y^{\phi 2j-1} f^{\psi 2j-1} \| y^{\phi 2j} f^{\psi 2j} \| G^{\phi 2j-1} H^{\eta 2j-1} \| G^{\phi 2j} H^{\eta 2j}$$

次に、有限体Ｚｑの元ｔ１, ｔ２, ｔ３, ｔ４, ｔ５をランダムに選び、それらを用いて、

$$T_1 := y^{t1} f^{t2} \bmod p$$

$$T_2 := f^{t2} g^{-t3} h^{-t4} e^{t5} \bmod p$$

$$T_3 := g^{t5} \bmod p$$

を計算する。

また、１≦ｊ≦ｋについて、有限体Ｚｑから乱数γjを、有限体Ｚｐから乱数u_jを選び、

$$e_j := e^{\gamma j} \bmod p$$

を計算する。また、

$g_j := g^{\gamma_j} \bmod p$

$J_j := G^{e_j} H^{u_j} \bmod P$

を計算する。

そして、これらの値から知識署名データ

$c := \mathcal{H}(g \| h \| f \| G \| H \| y \| e \| V_1 \| \cdots \| V_k \| T_1 \| T_2 \| T_3 \| g_1 \| \cdots \| g_k \| J_1 \| \cdots \| J_k \| m)$

、および、ｃ［ｊ］＝０のとき

$$v_{6j-5} := \phi_{2j-1}$$
$$v_{6j-4} := \phi_{2j}$$
$$v_{6j-3} := \psi_{2j-1}$$
$$v_{6j-2} := \psi_{2j}$$
$$v_{6j-1} := \eta_{2j-1}$$
$$v_{6j} := \eta_{2j}$$
$$w_j := \gamma_j \bmod q$$
$$z_j := u_j \bmod p$$

、ｃ［ｊ］＝１のとき、

$$v_{6j-5} := r_U + \phi_{2j-1}$$
$$v_{6j-4} := y^{\phi_{2j}} f^{\psi_{2j}}$$
$$v_{6j-3} := \omega + \psi_{2j-1}$$
$$v_{6j-2} := \psi_0 \in_U Z_q$$
$$v_{6j-1} := a + \eta_{2j-1}$$
$$v_{6j} := G^{\phi_{2j}} H^{\eta_{2j}}$$
$$w_j := \gamma_j - \tau \bmod q$$
$$z_j := u_j - a e_j r_U^{-1} \bmod p$$

を計算する。ここで、ｃ［ｊ］はｃのｊ番目のビットの値を表す。

ｃおよび（v_1，v_2，v_3，v_4，v_5，v_6，・・・，v_{6k-5}，v_{6k-4}，v_{6k-3}，v_{6k-2}，v_{6k-1}，v_{6k}）の部分は、メンバー証明書の第１の要素ｒを第２の乱数ωおよび第３の乱数ａを用いて正しく変換していることと、２つの式で変換されているｒが同じｒであることを証明する。つまり、

$h' = y^r f^\omega \bmod p$ かつ $J = G^r H^a \bmod P$ かつ $r \in [0, p-1]$

であることを示している。

cおよび（s1，s2，s3，s4，s5）の部分は、メンバー証明書（r，ξ）と署名鍵ωを正しく作成したことを証明する。つまり、

$e'h' = f^\omega g^{-\sigma} h^\xi e^r \bmod p$ かつ $h' = y^r f^\omega \bmod p$ かつ $g' = g^r \bmod p$

であることを示している。

cおよび（w_1，・・・，w_k，z_1，・・・，z_k）の部分は、第２の変換データＪで変換されたメンバー証明書の第１の要素ｒを暗号化データ（ｇ′，ｅ′）で正しく暗号化していることを証明する。つまり、

$J = G^r H^a \bmod P$ かつ $g' = g^r \bmod p$ かつ $e' = r^{-1} e^r \bmod p$

であることを示している。

最後に、署名出力手段２１０は、ステップＡ２０６で、暗号化データ（ｇ′，ｅ′）、第１の変換データｈ′、第２の変換データＪ、知識署名データ（ｃ，v_1，v_2，v_3，v_4，v_5，v_6，・・・v_{6k-5}，v_{6k-4}，v_{6k-3}，v_{6k-2}，v_{6k-1}，v_{6k}，s_1，s_2，s_3，s_4，s_5，w_1，・・・w_k，z_1，・・・z_k）をグループ署名として出力する。

検証手段３０１は、与えられたグループ署名が正しく作られたものであるか否かを確認する。この検証は、グループ署名に含まれる知識署名データを検証することにより行う。

知識署名データの検証では、与えられたグループ署名の署名者が、メンバー登録手段４０３と通信することで作成したメンバー証明書（ｒ，ξ）および署名鍵σを正しく所有しているか否かを確認することができる。しかし、グループ署名データ内では、メンバー証明書（ｒ，ξ）および署名鍵σは乱数を用いて秘匿されているので、登録された署名装置のうちどの装置が署名を作成したかの情報は検証を通じても得ることができない。

本実施の形態では、知識署名データの検証は、次の等式が成り立つか否かの確

認により行う。

$$c = \mathcal{H}\left(g \| h \| f \| G \| H \| y \| e \| V_1' \| \cdots \| V_k' \| T_1' \| T_2' \| T_3' \| g_1' \| \cdots \| g_k' \| J_1' \| \cdots \| J_k' \| m\right)$$

ここで、

$$V_j' = \begin{cases} y^{v_{6j-5}} f^{v_{6j-3}} \| y^{v_{6j-4}} f^{v_{6j-2}} \| & c[j] = 0 \\ G^{v_{6j-5}} H^{v_{6j-1}} \| G^{v_{6j-4}} H^{v_{6j}} & \\ y^{v_{6j-5}} f^{v_{6j-3}} / h' \| v_{6j-4} \| & c[j] = 1 \\ G^{v_{6j-5}} H^{v_{6j-1}} / J \| v_{6j} & \end{cases}$$

$$T_1' = h'^{c} y^{s_1} f^{s_2}$$

$$T_2' = (e'h')^{c} f^{s_2} g^{-s_3} h^{-s_4} e^{s_5}$$

$$T_3' = g'^{c} g^{s_5}$$

$$g_j' = g'^{c[j]} g^{w_j} \bmod p$$

$$J_j' = \begin{cases} G^{\bar{e}_j'} H^{z_j} \bmod P & c[j] = 0 \\ J^{\bar{e}_j'} H^{z_j} \bmod P & c[j] = 1 \end{cases}$$

$$(\text{where } \bar{e}_j' := e'^{c[j]} e^{w_j} \bmod p)$$

である。

そして、知識署名データが正しいことが確認できたら、そのグループ署名を受理する。知識署名データが正しくなければ、署名を不受理とする。

メンバー追跡装置５では、メンバー追跡手段５０３が、検証装置３０１で受理されたグループ署名の実際の署名者を特定する。

まず、メンバー追跡秘密情報記憶部５０２に記憶されたメンバー追跡秘密鍵εを用いて、

$$\bar{r} := g'^{\varepsilon} / e' \bmod p$$

を計算し、グループ署名の暗号化データ（ｇ′，ｅ′）から与えられた署名の署名者を表すメンバー証明書の第１の要素

$$\bar{r}$$

を復号する。また、それと同時に、メンバー追跡秘密情報記憶部５０２に記憶されたメンバー追跡秘密鍵εを用いて、復号結果

$\bar{r}$

が暗号化データ（ｇ′，ｅ′）をメンバー追跡秘密鍵εを用いて正しく復号した結果であることの証明データを次のように作成する。

有限体Ｚｑから乱数δを選び、

$$c := \mathcal{H}\left(g' \| e' \| \bar{r}^{-1} e' \| g'^{\delta}\right)$$

$$s := \delta - c\varepsilon \bmod q$$

を計算する。この（ｃ，ｓ）が証明データとなる。この証明データによる証明で、メンバー追跡装置５がグループ署名から

$\bar{r}$

を正しく復号したことが保証されることとなる。

次に、メンバー情報開示手段１０２に開示されたメンバーリスト｛$<I_U$，ｓｐｋ$_U$，ｒ，ξ，$S_U>$｝の中から、復号されたメンバー証明書の第１の要素

$\bar{r}$

と同一のメンバー証明書の第１の要素ｒを含むメンバーリスト（I_U，ｓｐｋ$_U$，ｒ，ξ，S_U）を検索する。検索できたら、合致したメンバーリストに対応する署名装置を、そのグループ署名の署名者であると特定する。

なお、本実施形態において、メンバー管理装置４とメンバー追跡装置５はグループ管理装置１の中に含まることとしてもよい。また、演算に用いている有限体上の乗法群の代わりに、楕円曲線上の有限群を用いることとしてもよい。

以上説明したように、本実施形態によれば、暗号化データ作成手段２０５、第１の変換データ作成手段２０６、および第２の変換データ作成手段２０７にて、メンバー証明書に関する情報を、後にグループ署名の要素として開示されることのない乱数を用いて秘匿しているので、メンバー追跡に必要な秘密情報を持たない装置はグループ署名データから署名者に関する情報を得ることができず、安全確実なグループ署名を提供することができ、また、メンバー管理装置４が署名者を特定することができず、グループ管理装置の機能をメンバー管理装置４とメンバー追跡装置５に安全に分割することができる。

次に、本発明の第２の実施形態について図面を参照して詳細に説明する。

図１２は、第２の実施形態のグループ署名システムの構成例を示すブロック図である。図１２を参照すると、第２の実施形態のグループ署名システムは、グループ管理装置１、署名装置２、検証装置３、第１～３のメンバーサブ管理装置６～８、第１～３のメンバーサブ追跡装置９～１１を有する。

本実施形態では、メンバーサブ管理装置およびメンバーサブ追跡装置をそれぞれ３つずつに分散する場合を例に説明するが、各装置の数に制限はない。第１～３のメンバーサブ管理装置６～８の間、および第１～３のメンバーサブ追跡装置間９～１１の間は、相互にブロードキャストチャネルで結ばれている。そして、第１～３のメンバーサブ管理装置６～８は、機能を分散して、グループメンバーの登録処理を行う。第１～３のメンバーサブ追跡装置９～１１は、機能を分散して、グループ署名から署名を作成したメンバーを特定する。

グループ管理装置１は、第１の実施形態と同様の構成を有し、システム全体で使用する公開情報を開示する。署名装置２は第１の実施形態と同様の構成を有している。また、検証装置３は第１の実施形態と同様の構成を有している。

第１～３のメンバーサブ管理装置６～８の各々は、分散離散対数鍵生成手段６０１，７０１，８０１、分散登録秘密情報記憶部６０２，７０２，８０２、分散メンバー登録手段６０３，７０３，８０３、および乱数生成器６０４，７０４，８０４を有している。以下簡単のため、メンバーサブ管理装置６について説明する。

分散離散対数鍵生成手段６０１は、他のメンバーサブ管理装置と通信を行いながら、分散メンバーサブ管理手段６０３で用いる分散登録秘密鍵を生成し、分散登録秘密情報記憶部６０２に出力する。

分散登録秘密情報記憶部６０２は、分散離散対数鍵生成手段６０１で生成した分散登録秘密鍵を記憶する。

分散メンバー登録手段６０３は、署名装置２と通信を行いながら、その署名装置２に対してメンバー証明書を発行する。ただし、分散メンバー登録手段６０３が出力するメンバー証明書は、単体ではメンバー証明書としての機能を持たない。署名装置２は各メンバー管理装置から受け取ったメンバー証明書から後に使用するメンバー証明書を計算することができる。

乱数生成器６０４は、分散離散対数鍵生成手段６０１および分散メンバー登録手段６０３で使用する乱数を生成する。

第１、第２、第３のメンバーサブ追跡装置９、１０、１１の各々は、分散離散対数鍵生成手段９０１，１００１，１１０１、分散追跡秘密情報記憶部９０２，１００２，１１０２、分散メンバー追跡手段９０３，１００３，１１０３、乱数生成器９０４，１００４，１１０４を有している。以下簡単のため、メンバーサブ追跡装置９について説明する。

分散離散対数鍵生成手段９０１は、他のメンバーサブ追跡装置と通信を行いながら、分散メンバー追跡手段９０３で用いる分散追跡秘密鍵を生成し、分散追跡秘密情報記憶部９０２に出力する。

分散追跡秘密情報記憶部９０２は、分散離散対数鍵生成装置９０１で生成した分散追跡秘密鍵を記憶する。

分散メンバー追跡手段９０３は、他のメンバーサブ追跡装置と通信を行いながら、検証装置３の検証手段３０１で受理されたグループ署名と、分散追跡秘密情報記憶部９０２に記憶された分散追跡秘密鍵と、メンバー情報開示手段１０２で開示されたメンバー情報とを入力として、グループ署名の署名者を特定し出力する。

乱数生成器９０４は、分散離散対数鍵生成手段９０１および分散メンバー追跡手段９０３で使用する乱数を生成する。

以下、第２の実施形態のグループ署名システムの詳細動作について説明する。

まず最初に前処理として、第１の実施形態と同様に、グループ管理装置１の前処理手段１０３が公開情報

$(p, q, P, g, h, f, G, H, \mathcal{H})$

を生成し、それを公開情報開示手段１０１が開示する。

次に、第１、第２、第３のメンバーサブ管理装置６、７、８の分散離散対数鍵生成手段６０１、７０１、８０１の各々が、メンバー登録に用いる公開鍵と分散秘密鍵を作成し、分散秘密鍵を分散登録秘密情報記憶部６０２、７０２、８０２に記録する。分散秘密鍵は、単体では秘密鍵としての役割を果たさないが、３つ

のメンバーサブ管理装置６、７、８の全てが正しく動作することにより、第１の実施形態のメンバー登録秘密鍵を使った処理と同様の機能を果たす。

本実施形態では、一例として、Ｐｅｄｅｒｓｅｎの“Ａ Ｔｈｒｅｓｈｏｌｄ Ｃｒｙｐｔｏｓｙｓｔｅｍ ｗｉｔｈｏｕｔ ａ Ｔｒｕｓｔｅｄ Ｐａｒｔｙ”（Ａｄｖａｎｃｅｓ ｉｎ Ｃｒｙｐｔｏｌｏｇｙ－ＥＵＲＯＣＲＹＰＴ‘９１，ｐｐ．５２２－５２６）に示された離散対数問題に基づく暗号系の分散秘密鍵生成方法に従った鍵生成手段を示す。

第１、第２、第３のメンバーサブ管理装置６、７、８の各々は、まず、Ｚｑ上の２次の多項式をランダムに選ぶ。ここで、第１のメンバーサブ管理装置６は多項式f_1（ｚ）を選ぶ。

$$f_1(z) = a_{10} + a_{11}z + a_{12}z^2 \bmod q$$

第２、第３のメンバーサブ管理装置７、８も、それと同様にf_2（ｚ）、f_3（ｚ）をそれぞれ選ぶ。

第１のメンバーサブ管理装置６は、

$$H_{11} = h^{a11} \bmod p,\ H_{12} = h^{a12} \bmod p,\ H_{13} = h^{a13} \bmod p$$

を第２のメンバーサブ管理装置７および第３のメンバーサブ管理装置８に送信する。

同様に、第２のメンバーサブ管理装置７はH_{21}，H_{22}，H_{23}を第１および第３のメンバーサブ管理装置６、８に送り、第３のメンバーサブ管理装置８はH_{31}，H_{32}，H_{33}を第１および第２のメンバーサブ管理装置６、７に送る。

ここでa_{10}，a_{20}，a_{30}をそれぞれυ_1，υ_2，υ_3と表記すると、υ_1，υ_2，υ_3がそれぞれのメンバーサブ管理装置６、７、８の分散登録秘密鍵となる。また、

$$y_1 = H_{10} = h^{\upsilon 1} \bmod p,\ y_2 = H_{20} = h^{\upsilon 2} \bmod p,\ y_3 = H_{30} = h^{\upsilon 3} \bmod p$$

が公開情報開示手段１０１に出力される。

そして、第１のメンバーサブ管理装置６は

$\overline{v}_{12} = f_1(2) \bmod q$

を第２のメンバーサブ管理装置７に、

$\overline{v}_{13} = f_1(3) \bmod q$

を第３のメンバーサブ管理装置８に、他の装置に内容を知られないよう秘密に、それぞれ送信する。

同様に、第２のメンバーサブ管理装置７は

$\overline{v}_{21} = f_2(1) \bmod q$

を第１のメンバーサブ管理装置６に、

$\overline{v}_{23} = f_2(3) \bmod q$

を第３のメンバーサブ管理装置８に、秘密に、送信する。また、第３のメンバーサブ管理装置７は

$\overline{v}_{31} = f_3(1) \bmod q$

を第１のメンバーサブ管理装置６に、

$\overline{v}_{32} = f_3(2) \bmod q$

を第２のメンバーサブ管理装置７に、秘密に、送信する。

これにより、第１のメンバーサブ管理装置６は、第２のメンバーサブ管理装置７からH_{21}，H_{32}，H_{23}および

$\overline{v}_{21}$

を、第３のメンバーサブ管理装置８からH_{31}，H_{32}，H_{33}および

$\overline{v}_{31}$

をそれぞれ受け取ることになる。

そして、第１のメンバーサブ管理装置６は他のメンバーサブ管理装置から受け取った

$\overline{v}_{21}$

および

$\overline{v}_{31}$

を検証する。この検証は次の等式を満たすか否かを確認することにより行なわれる。

$$h^{\bar{\upsilon}_{21}} = (H_{21})^{1^1} \cdot (H_{22})^{1^2} \cdot (H_{23})^{1^3} \bmod p$$
$$h^{\bar{\upsilon}_{31}} = (H_{31})^{1^1} \cdot (H_{32})^{1^2} \cdot (H_{33})^{1^3} \bmod p$$

メンバーサブ管理装置の各々は、この検証に失敗すると、その値の送り元のメンバーサブ管理装置に対して、検証失敗の旨を通知する。他の２つのメンバーサブ管理装置の双方から検証失敗の通知を受けたメンバーサブ管理装置は管理者としての資格を失う。

また、他のメンバーサブ管理装置のいずれか一方のみから検証失敗の通知を受けた場合、例えば、第１のメンバーサブ管理装置６のみが第２のメンバーサブ管理装置７の検証に失敗した場合には、第２のメンバーサブ管理装置７は、検証式を満たす

$\bar{\upsilon}_{21}$

を再び第１のメンバーサブ管理装置６に送信する。この

$\bar{\upsilon}_{21}$

が第１のメンバーサブ管理装置６にて検証式を満たさないとき、第２のメンバーサブ管理装置７は管理者としての資格を失う。第２のメンバーサブ管理装置７が資格を失った場合、$\upsilon_2 = 0$，$y_2 = 1$として、それ以降の処理を続ける。

メンバーサブ管理装置に共通のメンバー登録公開鍵ｙは、

$y = y_1 \cdot y_2 \cdot y_3 \cdot \mathrm{mod}\ p$

として計算する。つまり、各メンバーサブ管理装置６、７、８は、自身の分散登録秘密鍵が、素数を位数とする有限体の元を求めるための複数に分散された値のうちの自身に割り当てる１つであり、かつ、登録公開鍵が、その複数の分散登録秘密鍵から定まる元を離散対数とする値となるように、登録公開鍵と分散登録秘密鍵を求める。このとき、登録公開鍵は有限体上の乗法群の元となる。

そして、公開鍵ｙをグループ管理装置１の公開情報開示手段１０１に開示させ、第１、第２、第３のメンバーサブ管理装置６、７、８の各々は、υ_1，υ_2，υ_3を分散登録秘密鍵として、それぞれの分散登録秘密情報記憶部６０２、７０２、８０２に記憶する。

同様に、第１、第２、第３のメンバーサブ追跡装置９、１０、１１の分散離散

対数鍵生成手段９０１、１００１、１１０１は、メンバー追跡に用いる公開鍵と分散秘密鍵を作成する。そして、分散秘密鍵をメンバー追跡秘密鍵として、分散追跡秘密情報記憶部９０２、１００２、１１０２に記憶する。また、公開鍵をメンバー追跡公開鍵としてグループ管理装置１の公開情報開示手段１０１に開示させる。ここでメンバー追跡公開鍵はｅと表し、それぞれのメンバーサブ追跡装置が持つ秘密鍵をε_1，ε_2，ε_3と表す。

前処理および鍵生成の後、署名装置２は第１、第２、第３のメンバーサブ管理装置６、７、８との間で通信を行い、第１の実施形態と同様に、メンバー証明書（ｒ，ξ）および秘密鍵σを取得する。

署名装置２の登録手段２１３は、図１０のステップＡ１０１からＡ１０４と同様の動作により、第５の乱数生成器２１４で生成した有限体Ｚｑから選んだ乱数σを署名鍵とし、署名鍵の変換データI_U、知識署名データspk_U、および本人確認データS_Uを作成する。そして、署名装置２は変換データI_U、知識署名データspk_U、および本人確認データS_Uを第１、第２、第３のメンバーサブ管理装置６、７、８のすべてに送信する。

変換データI_U、知識署名データspk_U、および本人確認データS_Uを受け取った第１、第２、第３のメンバーサブ管理装置６、７、８はそれぞれ、図１０のステップＡ１０５と同様に、知識署名データspk_Uと本人確認データS_Uが正しいかどうか検証する。

それらの双方が検証を通過したら以降の処理を続ける。検証を通過しなければ処理が中断される。

検証の後、第１、第２、第３のメンバーサブ管理装置６、７、８は、分散メンバー管理秘密鍵の生成と同様に、有限体Ｚｑの元である乱数ｋに対応する分散情報k_1，k_2，k_3を計算する。また、第１のメンバーサブ管理装置６は

$$t_1 = h^{k_1} \bmod p$$

を、第２のメンバーサブ管理装置７は

$$t_2 = h^{k_2} \bmod p$$

を、第３のメンバーサブ管理装置８は

$$t_3 = h^{k_3} \bmod p$$

を公開情報開示手段１０１に出力する。また、

$t = t_1 \cdot t_2 \cdot t_3 \bmod p$

も公開情報開示手段１０１にて開示される。

次に、第１、第２、第３のメンバーサブ管理装置６、７、８は、公開情報ｔを用いて、メンバー証明書の第１の要素

$$r := I_U h^t \bmod p$$

を計算する。ｒは公開情報ｔを入力として計算されるため、すべてのメンバーサブ管理者で等しい値が得られる。また、分散生成した乱数k_1，k_2，k_3と分散登録秘密情報記憶部６０２、７０２、８０２に記憶された分散秘密鍵υ_1，υ_2，υ_3を用いて、第１、第２、第３のメンバーサブ管理装置６、７、８の各々は

$$\xi_1 = k_1 - r\upsilon_1 \bmod q \ , \ \xi_2 = k_2 - r\upsilon_2 \bmod q \ , \text{および} \ \xi_3 = k_3 - r\upsilon_3 \bmod q$$

の各々を計算する。そして、第１のメンバーサブ管理装置６は（ｒ，ξ_1）を、第２のメンバーサブ管理装置７は（ｒ，ξ_2）を、第３のメンバーサブ管理装置８は（ｒ，ξ_3）を署名装置２にそれぞれ送信する。

署名装置２は、受け取ったメンバー証明書（ｒ，ξ_1），（ｒ，ξ_2），（ｒ，ξ_3）が正しく作られているか否かを、

$$h^{\xi_1} = t_1 y_1^{-r} \bmod p \ , \ h^{\xi_2} = t_2 y_2^{-r} \bmod p \ , \text{および} \ h^{\xi_3} = t_3 y_3^{-r} \bmod p$$

が満たされるか否かを確認することにより検証する。この検証を通過したら、署名装置２は第１、第２、第３のメンバーサブ管理装置６、７、８にメンバー証明書を確認できた旨を通知する。その後、署名装置２は、第１、第２、第３のメンバーサブ管理装置６、７、８から受け取った全てのメンバー証明書の第２の要素を入力として、

$\xi = \xi_1 + \cdots + \xi_n$

を計算する。そして署名装置２は、（ｒ，ξ）をメンバー証明書としてメンバー情報記憶部２１２に記憶する。また、署名鍵σを秘密情報記憶部２１１に記憶する。

またメンバー管理装置４は、検証成功の通知を受けると、署名装置２を示すメンバーリストとして、署名装置２に送信したメンバー証明書、署名装置２から受け取った署名鍵の変換データ、知識署名データ、本人確認データをメンバー情報開示手段１０２に出力する。

本実施形態では、署名装置２における署名作成、検証装置３における署名検証は第１の実施形態と同様に行われる。

第１、第２、第３のメンバーサブ追跡装置９、１０、１１のメンバー追跡装置９０３、１００３、１１０３は次のように動作する。

第１、第２、第３のメンバーサブ追跡装置９、１０、１１は、まず、与えられたグループ署名に含まれる暗号化データ（ｇ′，ｅ′）の復号を行う。各メンバーサブ追跡装置９、１０、１１の各々は、分散追跡秘密情報記憶部９０２、１００２、１１０２の各々に記憶された分散追跡秘密鍵ε_1，ε_2，ε_3を用いて、

$$g'_1 := g'^{\varepsilon_1} \bmod p \ , \ g'_2 := g'^{\varepsilon_2} \bmod p \ , \ g'_3 := g'^{\varepsilon_3} \bmod p$$

をそれぞれ計算する。これらを用いて、

$$\bar{r} := g'^{\varepsilon} / e' = (g')^{\varepsilon_1+\varepsilon_2+\varepsilon_3} / e' = (g'_1 \cdot g'_2 \cdot g'_3) / e' \bmod p$$

を計算すると、与えられたグループ署名の署名者に該当するメンバー証明書の復号結果

$\bar{r}$

を得ることができる。そして、第１の実施形態と同様に、メンバー情報開示手段１０２に開示されたメンバーリスト{<I_U，spk_U，ｒ，ξ，S_U>}の中から、復号されたメンバー証明書の第１の要素

$\bar{r}$

と同一の、メンバー証明書の第１の要素ｒを含むメンバーリスト（I_U，spk_U，ｒ，ξ，S_U）を検索し、合致したメンバーリストに対応する署名装置２を署名者と特定する。

なお、本実施形態では、メンバーサブ管理装置およびメンバーサブ追跡装置が３つずつであり、これら全ての装置が正しく動作ったときに正しい処理が行われる。これを一般化して、メンバーサブ管理装置およびメンバーサブ追跡装置をｎ個ずつとした場合、

$t < n/2$

とおいて、鍵生成の際に第ｉのメンバーサブ管理装置もしくはメンバーサブ追跡装置が選ぶ多項式を

$$f_i(z) = a_{i0} + a_{i1}z + \ldots + a_{it}z^t \bmod q$$

とすれば、ｔ個以上のメンバーサブ管理装置もしくはメンバーサブ追跡装置が正しく動作したときにのみ、正しくメンバー登録および追跡処理を行うことができるものとなる。

以上説明したように、本実施形態によれば、メンバー管理装置の機能は複数のメンバーサブ管理装置に分散され、複数のメンバーサブ管理装置がメンバー証明書を計算するために使用する秘密鍵は、離散対数問題に基づく暗号系から選ばれるため、メンバーサブ管理装置の分散秘密鍵生成と分散メンバー登録処理の計算量が低減され、メンバーサブ管理装置の各々の負荷を低減することができる。

また、本実施形態によれば、メンバー追跡装置の機能は複数のメンバーサブ追跡装置に分散され、複数のメンバーサブ追跡装置が署名者の特定に用いる秘密鍵は、離散対数問題に基づく暗号系から選ばれるため、メンバーサブ管理装置の分散秘密鍵生成と署名者特定の分散した処理の計算量が低減され、メンバーサブ追跡装置の各々の負荷を低減することができる。

本発明によれば、署名装置が、メンバー証明書に関する情報を、グループ署名の要素として開示されない乱数を用いて秘匿するため、メンバー追跡に必要な秘密鍵を持たない装置はそれを解読できないので、特別な装置（メンバー追跡装置）以外はグループ署名から署名者を特定することができず、安全確実なグループ署名を提供することができる。また、メンバー登録を管理する機能と、グループ署名の署名者を特定する機能をグループ管理装置から分割する場合に、安全に分割することができる。また、メンバー管理装置の機能は複数のメンバーサブ管理装

置に分散され、複数のメンバーサブ管理装置がメンバー証明書を計算するために使用する秘密鍵は、離散対数問題に基づく暗号系から選ばれるため、メンバーサブ管理装置の分散秘密鍵生成と分散メンバー登録処理の計算量が低減され、メンバーサブ管理装置の各々の負荷を低減することができる。また、メンバー追跡装置の機能は複数のメンバーサブ追跡装置に分散され、複数のメンバーサブ追跡装置が署名者の特定に用いる秘密鍵は、離散対数問題に基づく暗号系から選ばれるため、メンバーサブ管理装置の分散秘密鍵生成と署名者特定の分散した処理の計算量が低減され、メンバーサブ追跡装置の各々の負荷を低減することができる。

請求の範囲

1． 署名者がグループに登録されたメンバーであることを証明することのできるグループ署名を作成し、グループ署名の署名者が前記グループのメンバーであるか否か確認するグループ署名システムであって、

システム内で共通に利用する公開情報を他の装置から参照可能に開示するグループ管理装置と、

第１の要素及び第２の要素を含むメンバー証明書の前記第１の要素を第１の乱数と前記グループ管理装置にて開示されている前記公開情報とを用いて暗号化して暗号化データを作成し、前記第１の要素を第２の乱数および前記公開情報を用いて変換して第１の変換データを作成し、前記第１の要素を第３の乱数および前記公開情報を用いて変換して第２の変換データを作成し、署名を付加すべきメッセージ、第４の乱数、前記暗号化データ、前記第１の変換データ、前記第２の変換データ、署名の作成に用いる秘密鍵である署名鍵、前記第１の要素、および前記第２の要素から、知識署名データを作成し、前記暗号化データ、前記第１の変換データ、前記第２の変換データ、および前記知識署名データをグループ署名として前記メッセージと共に出力する署名装置と、

メッセージおよびグループ署名と、前記グループ管理装置にて開示されている前記公開情報とから、前記グループ署名が、前記グループに登録されているいずれかのメンバーのメンバー証明書に含まれる第１の要素および第２の要素と前記署名鍵を用いて作成されたものか否かを検証する検証装置とを有するグループ署名システム。

2． 前記署名装置は、前記暗号化データ、前記第１の変換データ、および前記第２の変換データが同じ値を元に作成されていることを証明可能でありかつ前記第１の要素、前記第２の要素、および前記署名鍵に関する情報を知られることのないデータとして、前記知識署名データを作成し、

前記検証装置は、前記グループ署名が、前記グループに登録されているいずれかのメンバーのメンバー証明書に含まれる第１の要素および第２の要素と前記署

名鍵を用いて作成されたものか否かを、前記第１の要素、前記第２の要素、および前記署名鍵に関する情報を用いることなく、検証することを特徴とする請求項１に記載のグループ署名システム。

３．　新たなメンバーを前記グループに登録するとき、素数を位数とする有限体の元となるようにメンバー登録秘密鍵を選び、前記メンバー登録秘密鍵を離散対数とし、有限体上の乗法群の元であるメンバー登録公開鍵を前記メンバー登録秘密鍵から求め、前記メンバー登録公開鍵を公開情報として前記グループ管理装置に通知し、前記メンバー登録秘密鍵を自身で記憶すると共に、該メンバー登録秘密鍵を用いてメンバー証明書を作成し、前記署名装置に通知するメンバー管理装置をさらに有する、請求項１または請求項２に記載のグループ署名システム。

４．　前記メンバー証明書は、前記署名鍵を離散対数とする、前記署名鍵の変換データに対して前記メンバー登録秘密鍵を用いて作成したＮｙｂｅｒｇ－Ｒｕｅｐｐｅｌ署名である、請求項３に記載のグループ署名システム。

５．　前記グループ管理装置は、前記公開情報に加えて、前記メンバー管理装置から通知された前記メンバー情報を他の装置から参照可能に開示する、請求項３または請求項４に記載のグループ署名システム。

６．　新たなメンバーを前記グループに登録するとき、素数を位数とする有限体の所定の元の、複数に分散された値のうちの１つを自身の分散メンバー登録秘密鍵として割り当て、前記分散メンバー登録秘密鍵を自身で記憶すると共に、前記元を離散対数とする値をメンバー登録公開鍵とする、複数のメンバーサブ管理装置をさらに有し、

前記署名装置は、複数の前記メンバーサブ管理装置と通信することによりメンバー証明書を取得し、

前記グループ管理装置は、前記メンバー登録公開鍵を取得する、請求項１または請求項２に記載のグループ署名システム。

７．　素数を位数とする有限体の元となるようにメンバー追跡秘密鍵を選び、前記メンバー追跡秘密鍵を離散対数とし、有限体上の乗法群の元であるメンバー追跡公開鍵を前記メンバー追跡秘密鍵から求め、前記メンバー追跡公開鍵を前記公開情報として前記グループ管理装置に通知し、前記メンバー追跡秘密鍵を自身で記憶しておき、グループ署名の署名者を特定するとき、前記グループ署名に含まれている暗号化データを前記メンバー追跡秘密鍵を用いて復号し、復号結果と前記グループ管理装置にて開示されているいずれかの前記メンバー証明書の第１の要素とが一致すれば該メンバー証明書のメンバーを署名者と特定するメンバー追跡装置をさらに有し、

前記グループ管理装置は前記メンバー証明書を前記メンバー情報として開示しており、

前記署名装置は前記第１の要素を暗号化して前記暗号化データを作成するとき前記公開情報として前記メンバー追跡公開鍵を用いる、請求項１から請求項６のいずれか１項に記載のグループ署名システム。

８．　自身の分散メンバー追跡秘密鍵が、素数を位数とする有限体の元の複数に分散された値のうちの自身に割り当てる１つであり、メンバー追跡公開鍵が、前記有限体の元を離散対数とし、有限体上の乗法群の元となるように、前記分散メンバー追跡秘密鍵を求め、前記分散メンバー追跡秘密鍵を自身で記憶する複数のメンバーサブ追跡装置をさらに有し、

前記署名装置は前記第１の要素を暗号化して前記暗号化データを作成するとき前記公開情報として前記メンバー追跡公開鍵を用い、

前記グループ管理装置は前記メンバー証明書を前記メンバー情報として開示しており、

グループ署名の署名者を特定するとき、前記メンバーサブ追跡装置の各々が前記グループ署名に含まれている暗号化データに対して自身の前記分散メンバー追跡秘密鍵を用いて所定の計算をした結果から求まる復号結果と、前記グループ管理装置にて開示されているいずれかの前記メンバー証明書の第１の要素とが一致

すれば該メンバー証明書のメンバーを署名者と特定する、請求項１から請求項６のいずれか１項に記載のグループ署名システム。

９．　前記有限体上の乗法群に代えて楕円曲線上の有限群を用いる、請求項３、６、７、８のいずれか１項に記載のグループ署名システム。

１０．　グループ管理装置、署名装置、および検証装置を有するグループ署名システムにおいて、署名者がグループに登録されたメンバーであることを証明することのできるグループ署名を作成し、グループ署名の署名者が前記グループのメンバーであるか否か確認するためのグループ署名方法であって、

前記グループ管理装置において、

システム内で共通に利用する公開情報を他の装置から参照可能に開示するステップと、

前記署名装置において、

第１の要素および第２の要素を含むメンバー証明書を記憶するステップと、

前記第１の要素を第１の乱数と前記グループ管理装置にて開示されている前記公開情報とを用いて暗号化して暗号化データを作成するステップと、

前記第１の要素を第２の乱数および前記公開情報を用いて変換して第１の変換データを作成するステップと、

前記第１の要素を第３の乱数および前記公開情報を用いて変換して第２の変換データを作成するステップと、

署名を付加すべきメッセージ、第４の乱数、前記暗号化データ、前記第１の変換データ、前記第２の変換データ、署名の作成に用いる秘密鍵である署名鍵、前記第１の要素、および前記第２の要素から、前記暗号化データ、前記第１の変換データ、および前記第２の変換データが同じ値を元に作成されていることを証明可能でありかつ前記第１の要素、前記第２の要素、および前記署名鍵に関する情報を知られることのない知識署名データを作成するステップと、

前記暗号化データ、前記第１の変換データ、前記第２の変換データ、および前記知識署名データをグループ署名として前記メッセージと共に出力するステップ

と、

前記検証装置において、

メッセージおよびグループ署名と、前記グループ管理装置にて開示されている前記公開情報とから、前記グループ署名が、前記グループに登録されているいずれかのメンバーのメンバー証明書に含まれる第１の要素および第２の要素と前記署名鍵を用いて作成されたものか否かを、前記第１の要素、前記第２の要素、および前記署名鍵に関する情報を用いることなく検証するステップとを有するグループ署名方法。

１１．　システム内で共通に利用する公開情報を他の装置から参照可能に開示するグループ管理装置、およびグループ署名の署名者がグループのメンバーであるか否か確認する検証装置と共にグループ署名システムを構成し、前記署名者が前記グループに登録されたメンバーであることを証明することのできるグループ署名を作成するグループ署名装置であって、

第１の要素および第２の要素を含むメンバー証明書を記憶するメンバー情報記憶手段と、

前記第１の要素を第１の乱数と前記グループ管理装置にて開示されている前記公開情報とを用いて暗号化して暗号化データを作成する暗号化データ作成手段と、

前記第１の要素を第２の乱数および前記公開情報を用いて変換して第１の変換データを作成する第１の変換データ作成手段と、

前記第１の要素を第３の乱数および前記公開情報を用いて変換して第２の変換データを作成する第２の変換データ作成手段と、

署名を付加すべきメッセージ、第４の乱数、前記暗号化データ、前記第１の変換データ、前記第２の変換データ、署名の作成に用いる秘密鍵である署名鍵、前記第１の要素、および前記第２の要素から、前記暗号化データ、前記第１の変換データ、および前記第２の変換データが同じ値を元に作成されていることを証明可能でありかつ前記第１の要素、前記第２の要素、および前記署名鍵に関する情報を知られることのない知識署名データを作成する知識署名作成手段と、

前記暗号化データ、前記第１の変換データ、前記第２の変換データ、および前

記知識署名データをグループ署名として前記メッセージと共に出力する署名出力手段とを有するグループ署名装置。

１２．　システム内で共通に利用する公開情報を他の装置から参照可能に開示するグループ管理装置、およびグループ署名の署名者がグループのメンバーであるか否か確認する検証装置と共にグループ署名システムを構成するグループ署名装置として動作させ、前記署名者が前記グループに登録されたメンバーであることを証明することのできるグループ署名を作成させるために、コンピュータに実行させるグループ署名プログラムであって、

メンバー情報記憶手段が、第１の要素および第２の要素を含むメンバー証明書を記憶する処理と、

暗号化データ作成手段が、前記第１の要素を第１の乱数と前記グループ管理装置にて開示されている前記公開情報とを用いて暗号化して暗号化データを作成する処理と、

第１の変換データ作成手段が、前記第１の要素を第２の乱数および前記公開情報を用いて変換して第１の変換データを作成する処理と、

第２の変換データ作成手段が、前記第１の要素を第３の乱数および前記公開情報を用いて変換して第２の変換データを作成する処理と、

知識署名作成手段が、署名を付加すべきメッセージ、第４の乱数、前記暗号化データ、前記第１の変換データ、前記第２の変換データ、署名の作成に用いる秘密鍵である署名鍵、前記第１の要素、および前記第２の要素から、前記暗号化データ、前記第１の変換データ、および前記第２の変換データが同じ値を元に作成されていることを証明可能でありかつ前記第１の要素、前記第２の要素、および前記署名鍵に関する情報を知られることのない知識署名データを作成する処理と、

署名出力手段が、前記暗号化データ、前記第１の変換データ、前記第２の変換データ、および前記知識署名データをグループ署名として前記メッセージと共に出力する処理とを有するグループ署名プログラム。

図１

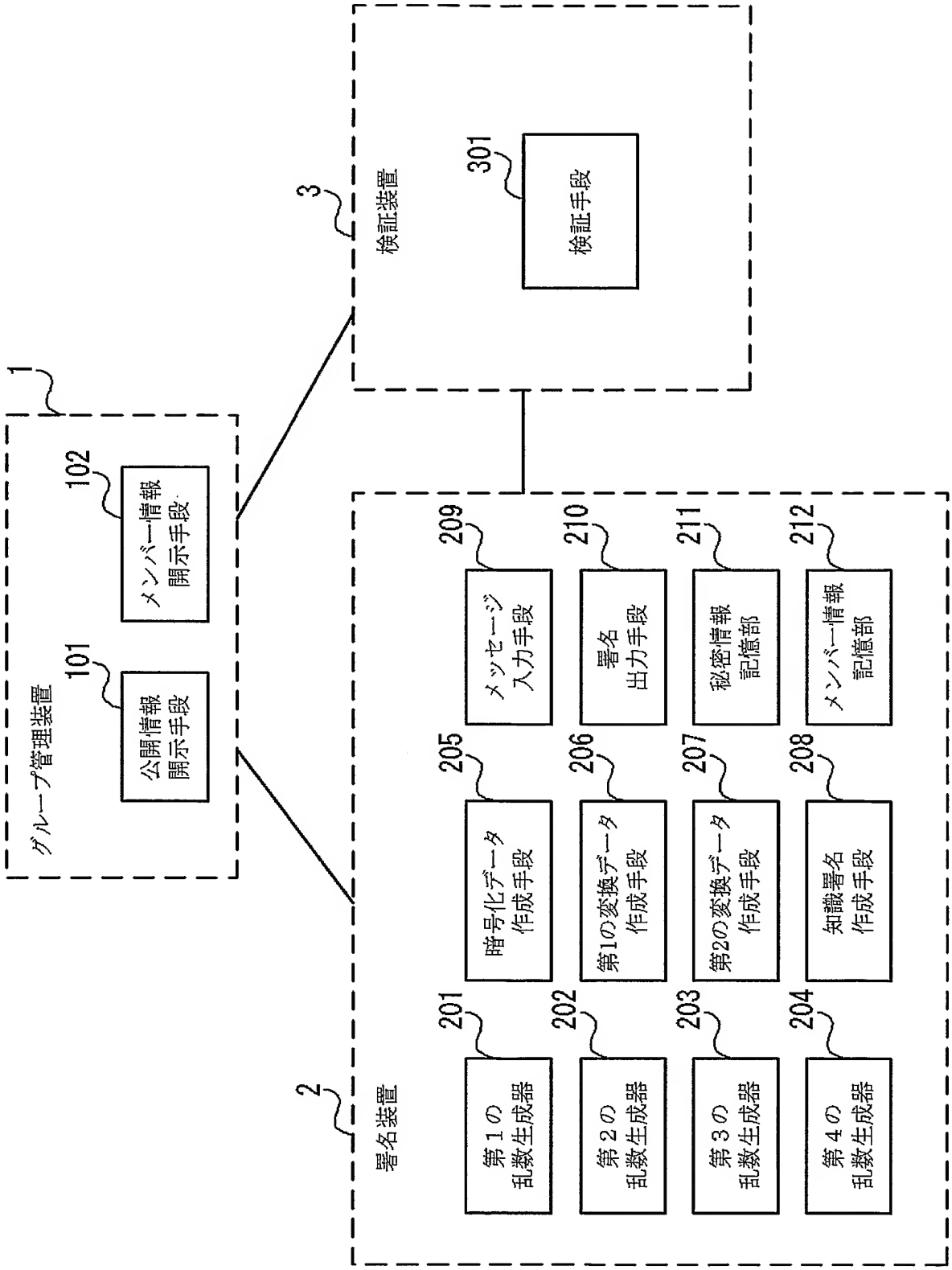

1
グループ管理装置
101
公開情報
開示手段
102
メンバー情報
開示手段
2
署名装置
201
第１の
乱数生成器
202
第２の
乱数生成器
203
第３の
乱数生成器
204
第４の
乱数生成器
205
暗号化データ
作成手段
206
第1の変換データ
作成手段
207
第2の変換データ
作成手段
208
知識署名
作成手段
209
メッセージ
入力手段
210
署名
出力手段
211
秘密情報
記憶部
212
メンバー情報
記憶部
3
検証装置
301
検証手段

図２

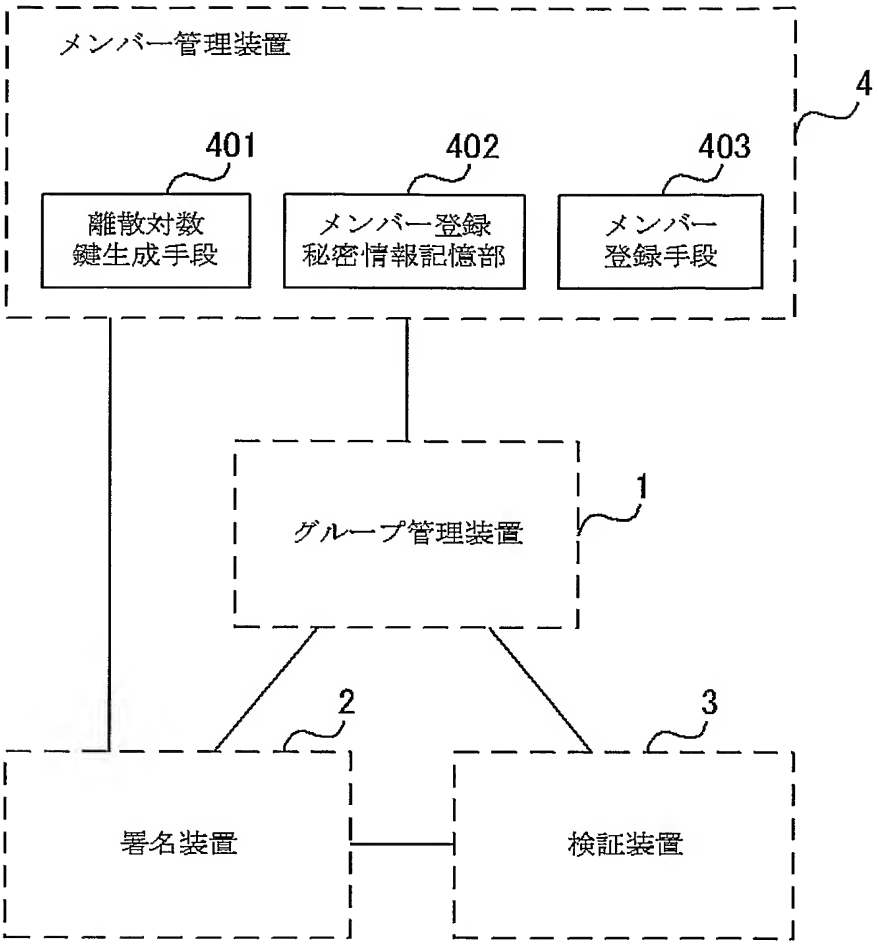

メンバー管理装置
4
401
402
403
離散対数
鍵生成手段
メンバー登録
秘密情報記憶部
メンバー
登録手段
グループ管理装置
1
2
3
署名装置
検証装置

図 3

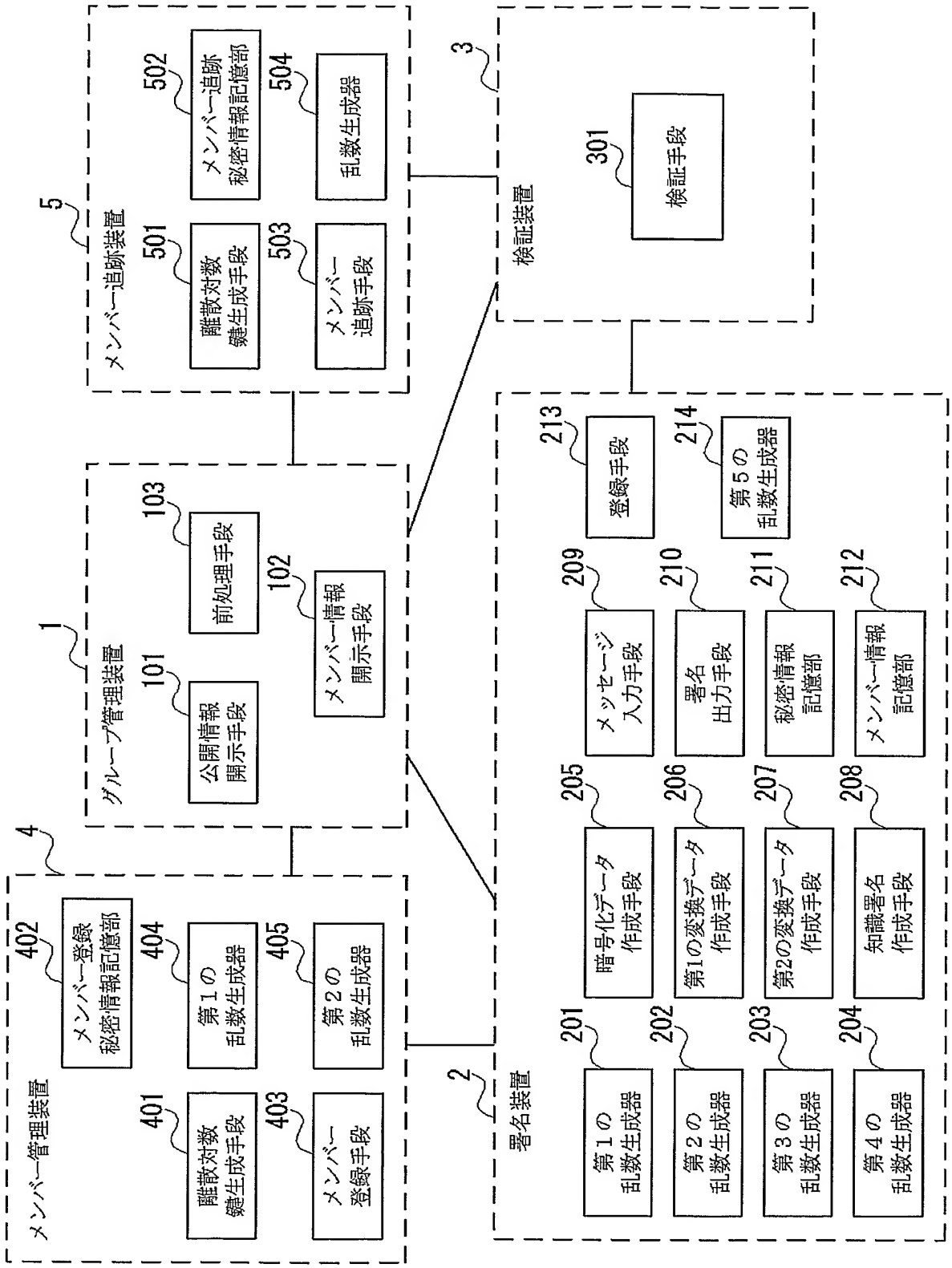

メンバー管理装置
4
メンバー登録秘密情報記憶部
402
離散対数鍵生成手段
401
メンバー登録手段
403
第１の乱数生成器
404
第２の乱数生成器
405
グループ管理装置
1
公開情報開示手段
101
前処理手段
103
メンバー情報開示手段
102
メンバー追跡装置
5
メンバー追跡秘密情報記憶部
502
離散対数鍵生成手段
501
メンバー追跡手段
503
乱数生成器
504
検証装置
3
検証手段
301
署名装置
2
第１の乱数生成器
201
第２の乱数生成器
202
第３の乱数生成器
203
第４の乱数生成器
204
暗号化データ作成手段
205
第1の変換データ作成手段
206
第2の変換データ作成手段
207
知識署名作成手段
208
メッセージ入力手段
209
署名出力手段
210
秘密情報記憶部
211
メンバー情報記憶部
212
登録手段
213
第５の乱数生成器
214

図４

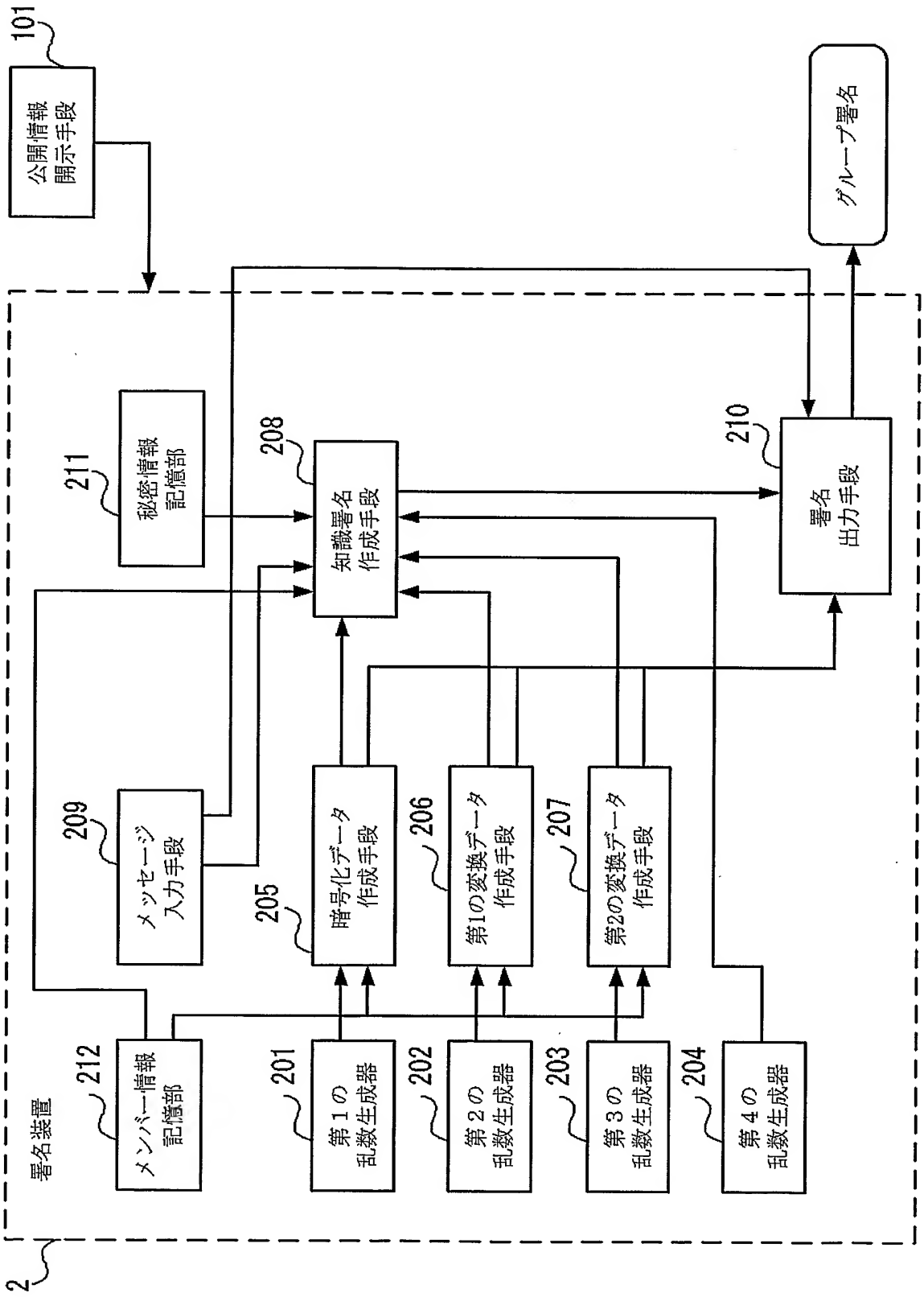

101
公開情報
開示手段
グループ署名
署名装置
2
秘密情報
記憶部
211
208
知識署名
作成手段
210
署名
出力手段
メッセージ
入力手段
209
暗号化データ
作成手段
205
第1の変換データ
作成手段
206
第2の変換データ
作成手段
207
メンバー情報
記憶部
212
第１の
乱数生成器
201
第２の
乱数生成器
202
第３の
乱数生成器
203
第４の
乱数生成器
204

図5

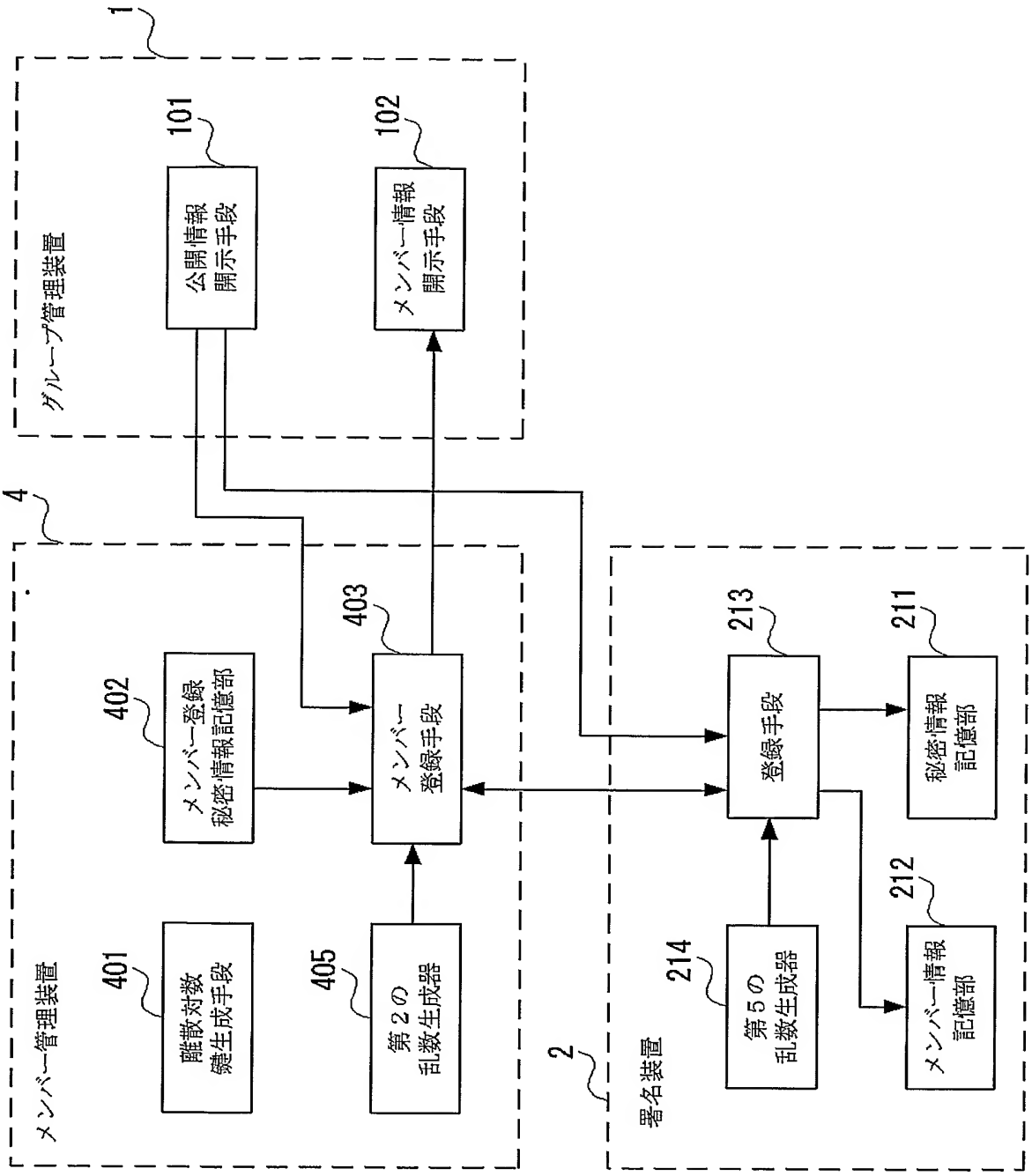

1
グループ管理装置
101
公開情報
開示手段
102
メンバー情報
開示手段
4
メンバー管理装置
402
メンバー登録
秘密情報記憶部
403
メンバー
登録手段
401
離散対数
鍵生成手段
405
第2の
乱数生成器
2
署名装置
213
登録手段
211
秘密情報
記憶部
212
メンバー情報
記憶部
214
第5の
乱数生成器

図６

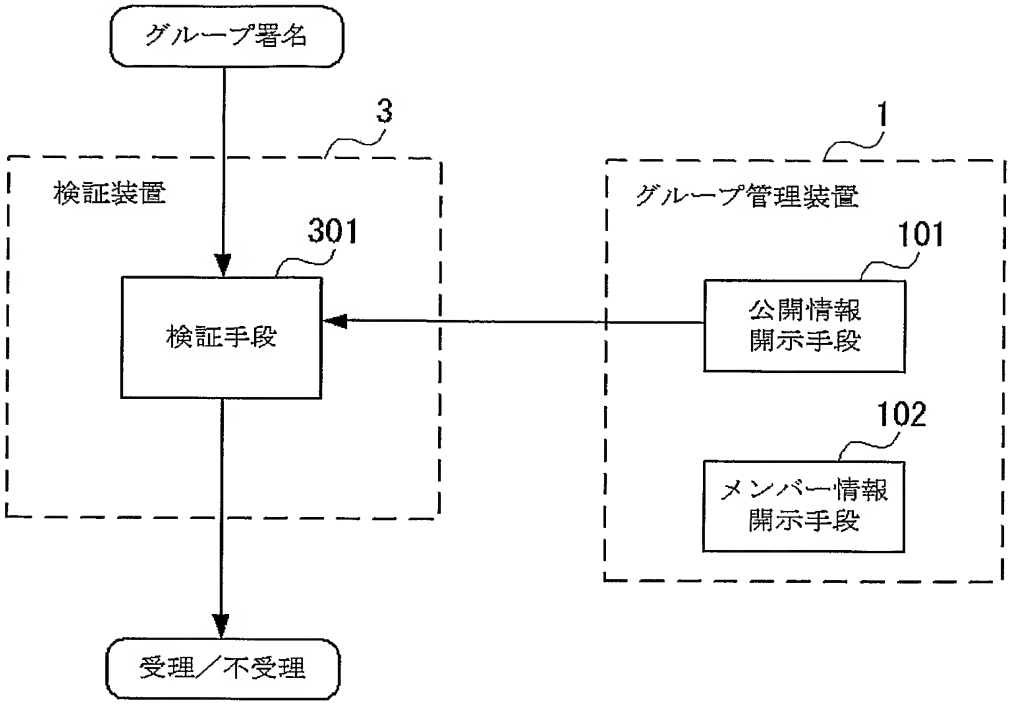

グループ署名
3
検証装置
301
検証手段
1
グループ管理装置
101
公開情報
開示手段
102
メンバー情報
開示手段
受理／不受理

図７

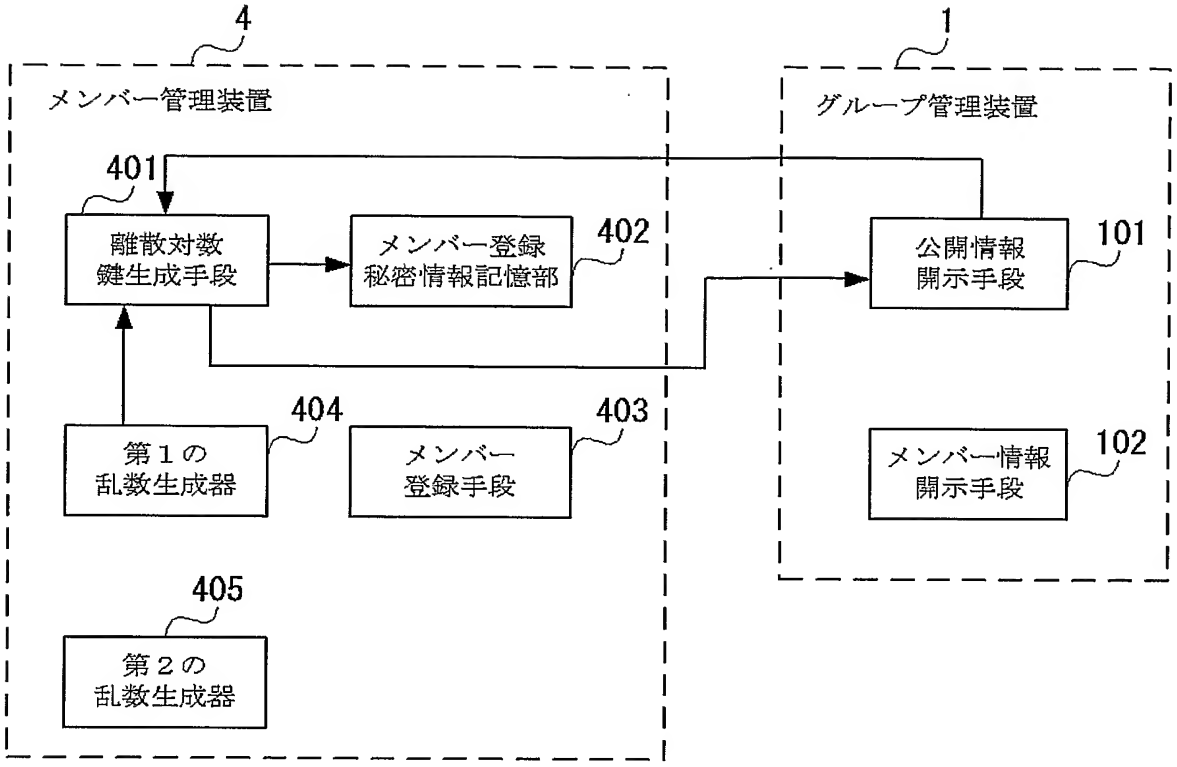

4
メンバー管理装置
401
離散対数
鍵生成手段
メンバー登録
秘密情報記憶部
402
第１の
乱数生成器
404
メンバー
登録手段
403
405
第２の
乱数生成器
1
グループ管理装置
公開情報
開示手段
101
メンバー情報
開示手段
102

図８

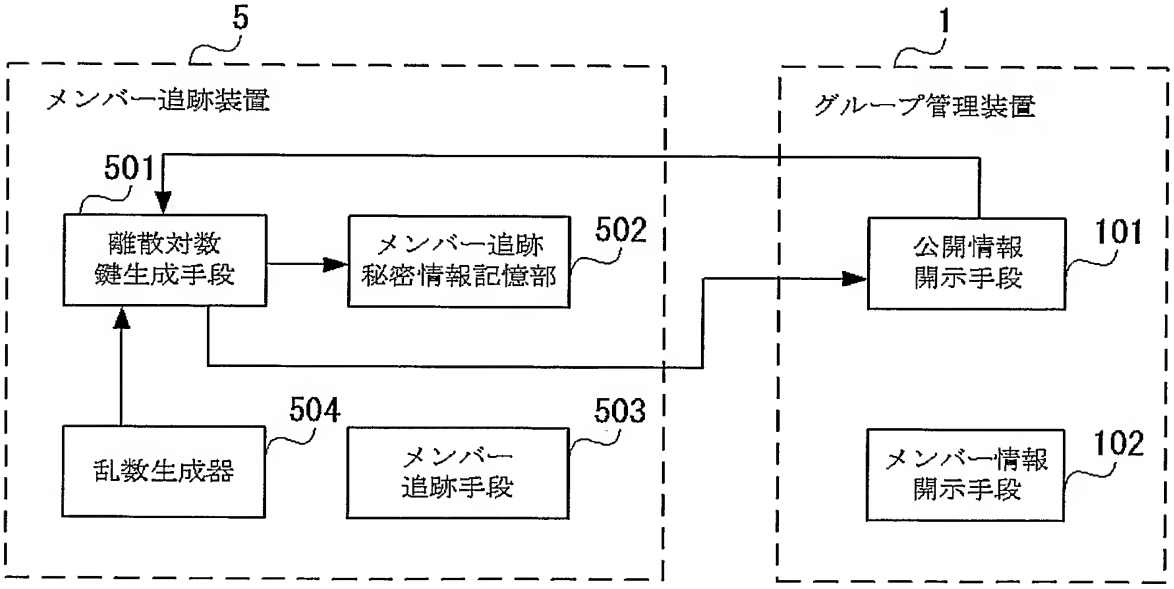

5
メンバー追跡装置
501
離散対数
鍵生成手段
メンバー追跡
秘密情報記憶部
502
乱数生成器
504
メンバー
追跡手段
503
1
グループ管理装置
公開情報
開示手段
101
メンバー情報
開示手段
102

図９

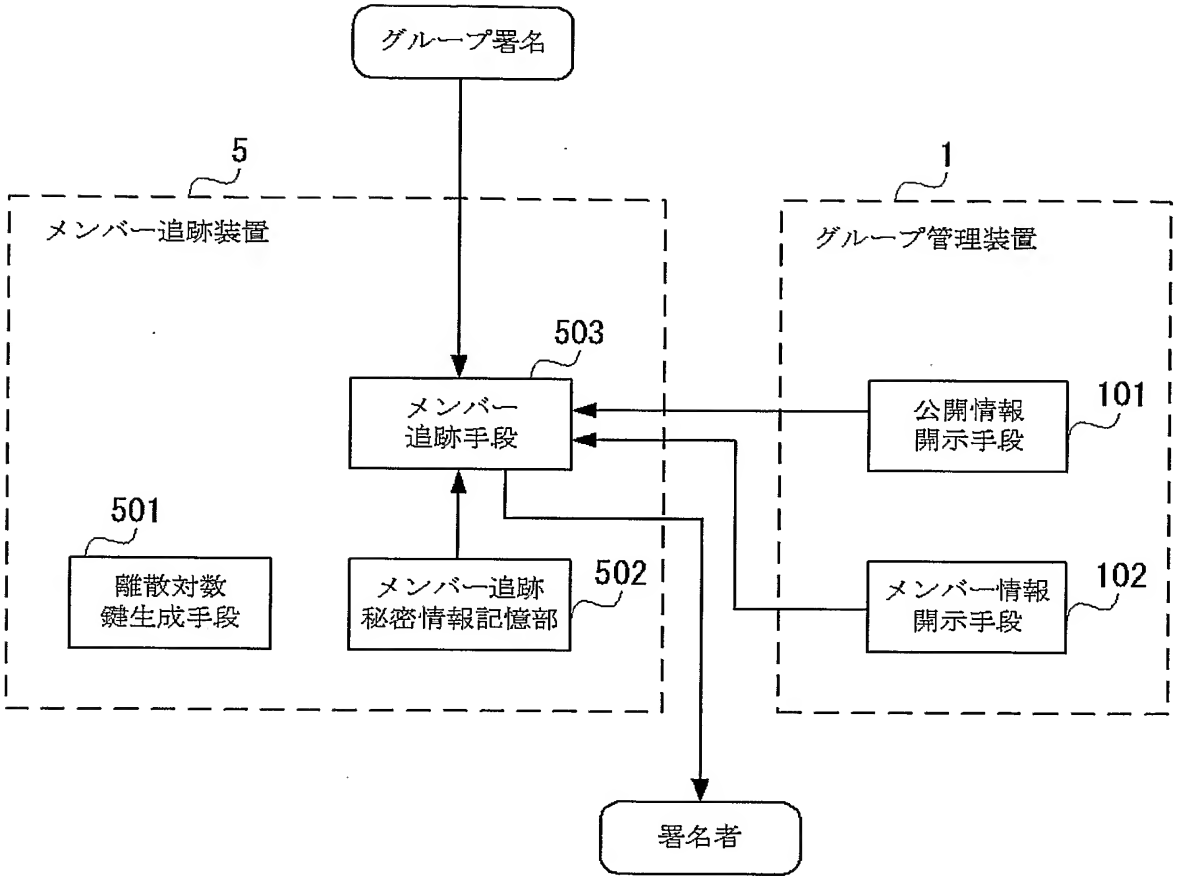

グループ署名
5
メンバー追跡装置
1
グループ管理装置
503
メンバー
追跡手段
公開情報
開示手段
101
501
離散対数
鍵生成手段
メンバー追跡
秘密情報記憶部
502
メンバー情報
開示手段
102
署名者

図１０

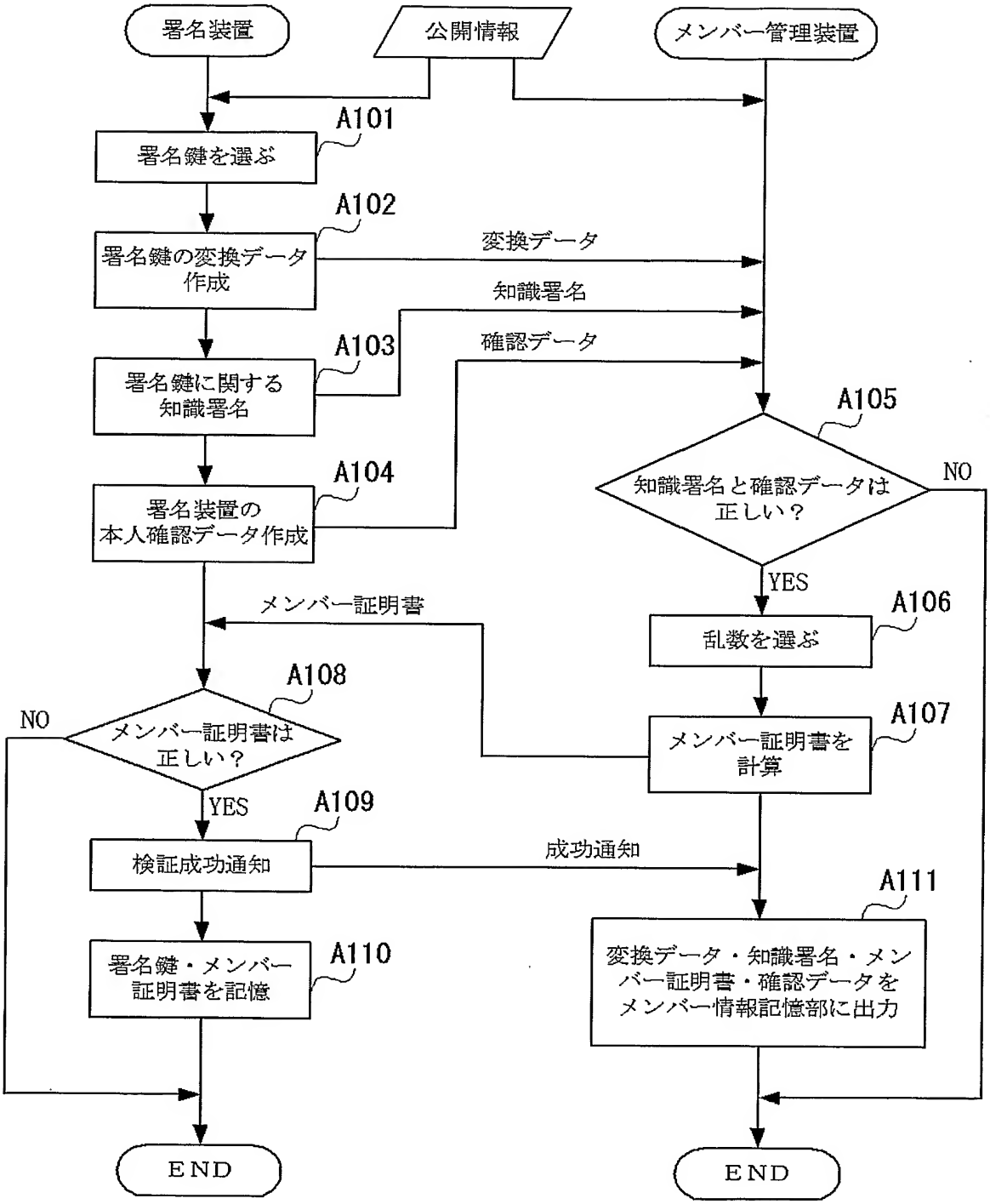

署名装置
公開情報
メンバー管理装置
A101
署名鍵を選ぶ
A102
署名鍵の変換データ作成
変換データ
知識署名
確認データ
A103
署名鍵に関する知識署名
A104
署名装置の本人確認データ作成
A105
知識署名と確認データは正しい？
NO
YES
A106
乱数を選ぶ
メンバー証明書
A107
メンバー証明書を計算
A108
メンバー証明書は正しい？
NO
YES
A109
検証成功通知
成功通知
A110
署名鍵・メンバー証明書を記憶
A111
変換データ・知識署名・メンバー証明書・確認データをメンバー情報記憶部に出力
END
END

図１１

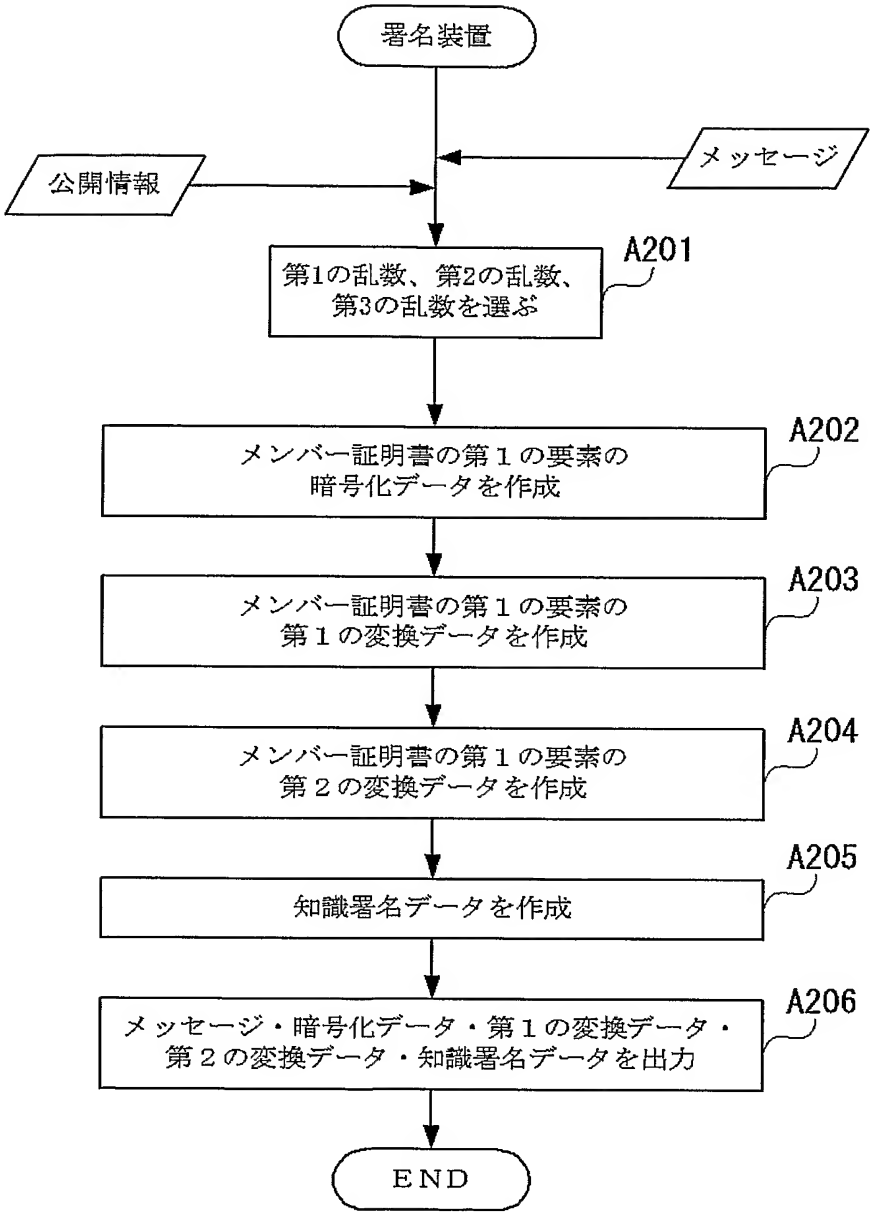

署名装置
公開情報
メッセージ
第1の乱数、第2の乱数、
第3の乱数を選ぶ
A201
メンバー証明書の第１の要素の
暗号化データを作成
A202
メンバー証明書の第１の要素の
第１の変換データを作成
A203
メンバー証明書の第１の要素の
第２の変換データを作成
A204
知識署名データを作成
A205
メッセージ・暗号化データ・第１の変換データ・
第２の変換データ・知識署名データを出力
A206
END

図１２

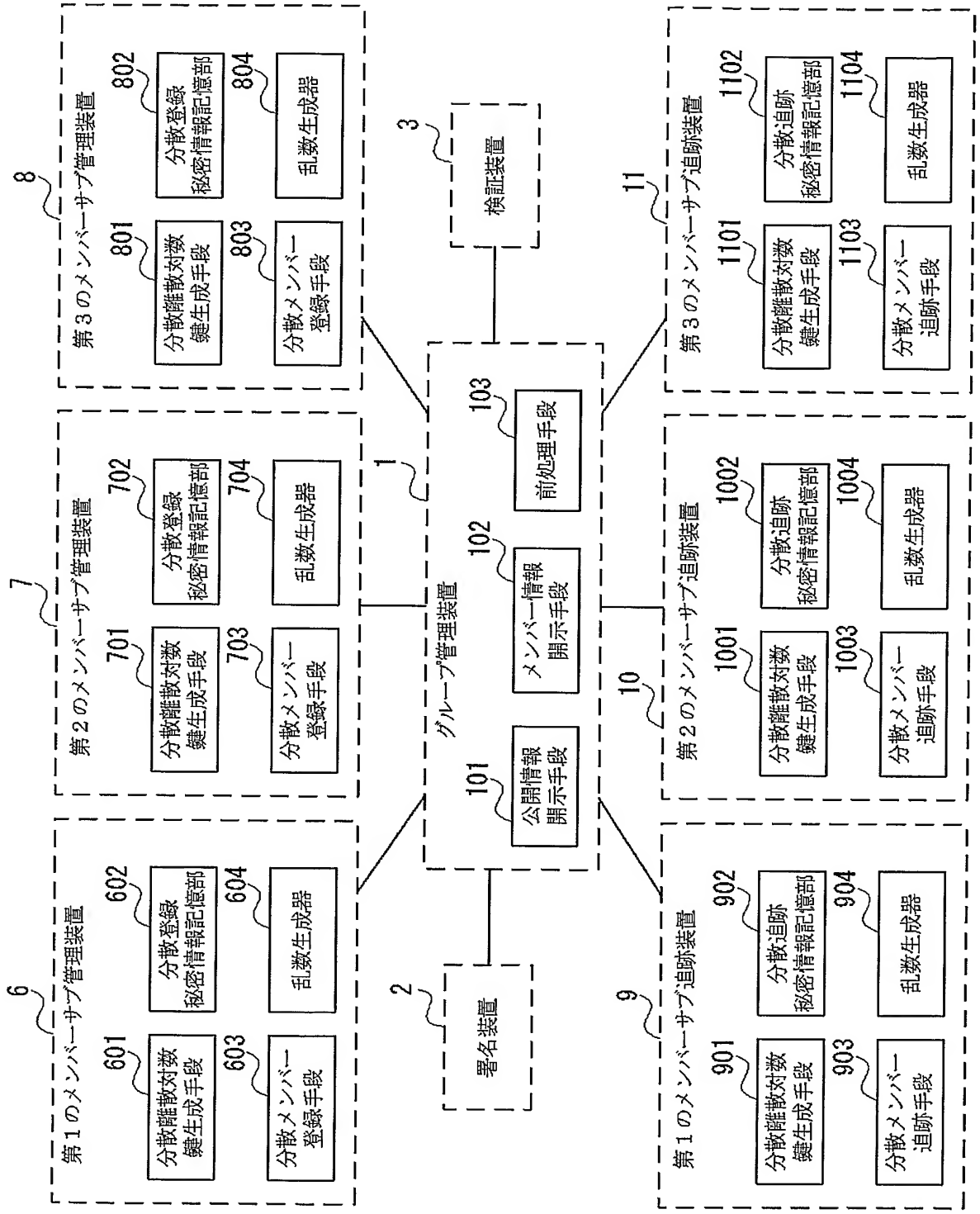
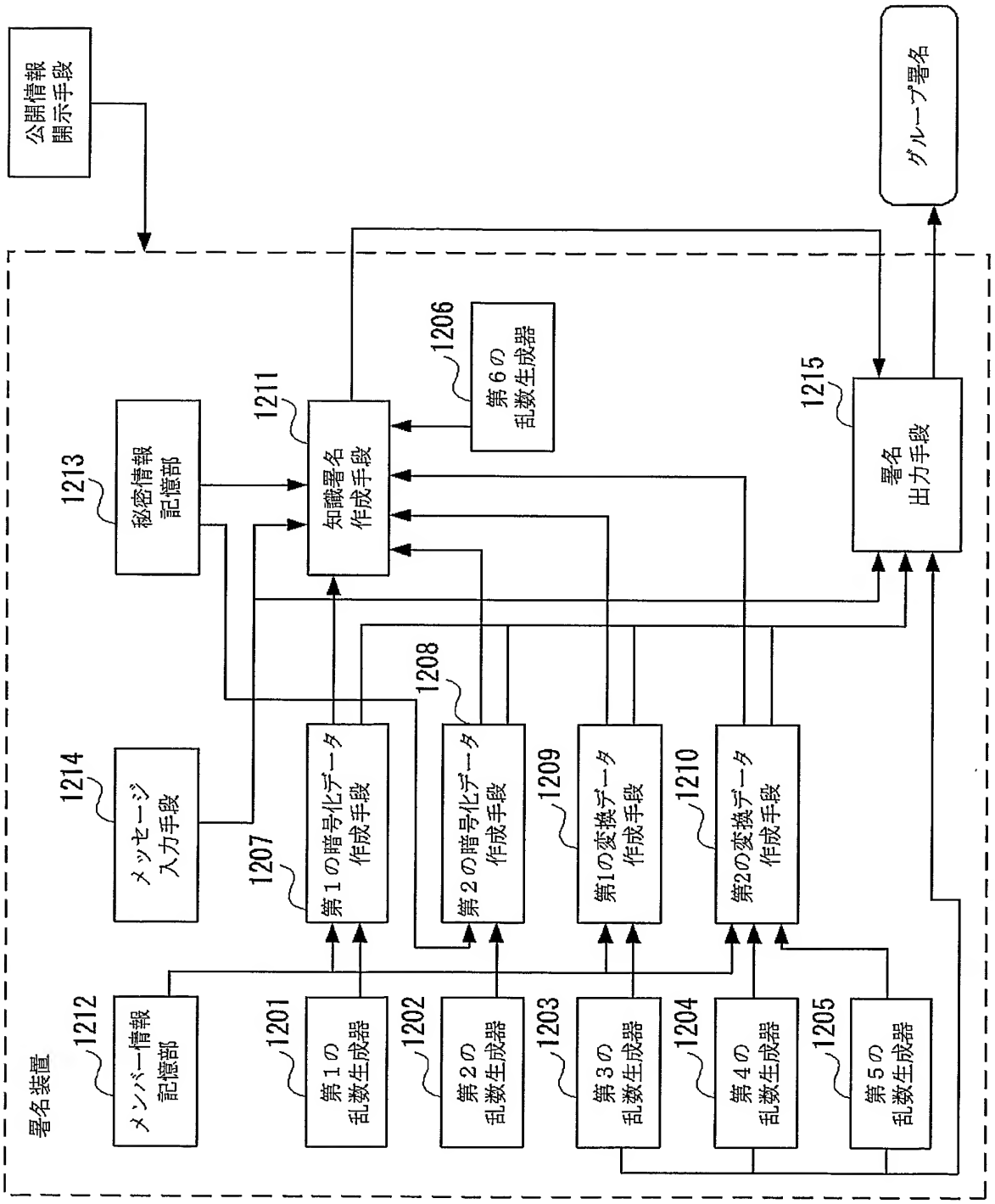

グループ管理装置
1
公開情報開示手段
101
メンバー情報開示手段
102
前処理手段
103
署名装置
2
検証装置
3
第１のメンバーサブ管理装置
6
分散離散対数鍵生成手段
601
分散登録秘密情報記憶部
602
分散メンバー登録手段
603
乱数生成器
604
第２のメンバーサブ管理装置
7
分散離散対数鍵生成手段
701
分散登録秘密情報記憶部
702
分散メンバー登録手段
703
乱数生成器
704
第３のメンバーサブ管理装置
8
分散離散対数鍵生成手段
801
分散登録秘密情報記憶部
802
分散メンバー登録手段
803
乱数生成器
804
第１のメンバーサブ追跡装置
9
分散離散対数鍵生成手段
901
分散追跡秘密情報記憶部
902
分散メンバー追跡手段
903
乱数生成器
904
第２のメンバーサブ追跡装置
10
分散離散対数鍵生成手段
1001
分散追跡秘密情報記憶部
1002
分散メンバー追跡手段
1003
乱数生成器
1004
第３のメンバーサブ追跡装置
11
分散離散対数鍵生成手段
1101
分散追跡秘密情報記憶部
1102
分散メンバー追跡手段
1103
乱数生成器
1104

図１３


公開情報
開示手段
グループ署名
署名装置
メンバー情報
記憶部
1212
第１の
乱数生成器
1201
第２の
乱数生成器
1202
第３の
乱数生成器
1203
第４の
乱数生成器
1204
第５の
乱数生成器
1205
メッセージ
入力手段
1214
第１の暗号化データ
作成手段
1207
第２の暗号化データ
作成手段
1208
第1の変換データ
作成手段
1209
第2の変換データ
作成手段
1210
秘密情報
記憶部
1213
知識署名
作成手段
1211
第６の
乱数生成器
1206
署名
出力手段
1215

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001177

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/32, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/32, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Jitsuyo Shinan Toroku Koho 1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), WPI, INSPEC(DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Kozue Umeda, Atsuko Miyaji, "A Group Signature Scheme based on Nyberg-Ryeppel Signatures", 2003 Nen Ango to Joho Security Symposium Yokoshu, Vol.1 of 2, 26 January, 2003 (26.01.03), pages 327 to 332	1-12
Y	Takamitsu KATO, Shoichi HIROSE, Michihiko MINO, Katsuo IKEDA, "ElGamal no Kokai Kagi Angokei ni Motozuku Group Shomei ni yoru Shomei Protocol", 1992 Nen The Institute of Electronics, Information and Communication Engineers - Soritsu 75 Shunen Kinen - Shuki Taikai Koen Ronbunshu, separate Vol.1, 15 September, 1992 (15.09.92), page 1·187	1-12

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 April, 2005 (26.04.05)	17 May, 2005 (17.05.05)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001177

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	Shoko YONEZAWA, Jun FURUKAWA, "Kanrisha Bunsan ni Tekishita Group Shomei Hoshiki", 2004 Nen Ango to Joho Security Symposium Yokoshu, Vol.2 of 2, 27 January, 2004 (27.01.04), pages 1167 to 1172	1-12

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／００１１７７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／３２，Ｇ０９Ｃ１／００

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／３２，Ｇ０９Ｃ１／００

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国登録実用新案公報	１９９４－２００５年
日本国実用新案登録公報	１９９６－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

ＪＩＣＳＴファイル（ＪＯＩＳ），ＷＰＩ，ＩＮＳＰＥＣ（ＤＩＡＬＯＧ）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	Kozue Umeda, Atsuko Miyaji, “A Group Signatue Scheme based on Nyberg-Ryeppel Signatures”，２００３年暗号と情報セキュリティシンポジウム予稿集，Ｖｏｌｕｍｅ　１　ｏｆ　２，２００３．０１．２６，ｐ．３２７－３３２	１－１２
Ｙ	加藤隆充，廣瀬勝一，美濃導彦，池田克夫，“Ｅｌ Ｇａｍａｌの公開鍵暗号系に基づくグループ署名による署名プロトコル”，１９９２年電子情報通信学会一創立７５周年記念一秋季大会講演論文集，分冊１，１９９２．０９．１５，ｐ．１・１８７	１－１２

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日　２６．０４．２００５	国際調査報告の発送日　17. 5. 2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｍ　４２２９ 青木　重徳 電話番号　０３－３５８１－１１０１　内線　３５９７

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｐ，Ｘ	米沢祥子，古川潤，“管理者分散に適したグループ署名方式”，２００４年暗号と情報セキュリティシンポジウム予稿集，Ｖｏｌｕｍｅ　２　ｏｆ　２，２００４．０１．２７，ｐ．１１６７－１１７２	１－１２